Departamento de Informática

Ingeniería Técnica en Informática de Gestión

PROYECTO FIN DE CARRERA

ANÁLISIS DEL DOMINIO DE CONTROL DE ACCESOS DE LA ISO/IEC 27002:2013 Y MÉTRICAS PARA CUADROS DE MANDO

Autor: María Elena Martínez Bernardo

Tutor: Miguel Ángel Ramos González

Leganés, Septiembre de 2015

Título: ANÁLISIS DEL DOMINIO DE CONTROL DE ACCESOS DE LA ISO/IEC 27002:2013 Y MÉTRICAS PARA CUADROS DE MANDO

Autor: María Elena Martínez Bernardo

Director: Miguel Ángel Ramos González

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de _____.

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

En primer lugar quiero agradecer al tutor de este proyecto, Don Miguel Angel Ramos González, el haber aceptado acompañarme en la elaboración de este proyecto fin de carrera. Sin querer entrar a dar detalles, pero ha sido un acto de corazón y precisamente por eso mi gratitud y mi primer agradecimiento para él.

En segundo lugar, a mí marido, Antonio, que nunca ha desistido en que encontraríamos ese hueco para hacer realidad que tenemos el título de ingenieros en informática de gestión. Gracias, gracias y más gracias.

En tercer lugar a mis padres, Ernesto y Mayte y mis suegros, Antonio y Mari, porque su tiempo, ganas y paciencia es el que ha permitido que yo pudiera también tener tiempo (y fuerzas) para hacer este proyecto.

Y por último a mis dos chiquitines, Alejandro de 5 años e Irene de 3 años, que con lo pequeños que son, entendían que mamá tenía que trabajar haciendo este proyecto ¿se imaginan?. Sus abrazos sí que dan fuerzas para comerse el mundo.

Gracias de corazón a todos. Uno es la suma de los que le rodean.

Resumen

Este proyecto fin de carrera se centra en uno de los dominios que trata la versión del 2013 del estándar ISO/IEC 27002, el dominio de Control de Accesos.

Dicho estándar define una serie de objetivos y en base a ellos una serie de controles de seguridad que son unas pautas de mínimos que cualquier organización, independientemente de su tamaño y sector de actividad, debería tener en cuenta. Aunque la aplicación de controles concretos de seguridad no es una garantía de que se previenen el 100% de los ataques o fallos de seguridad, su aplicación sí minimiza enormemente la aparición de éstos y más, cuando se complementa con un modelo de gestión continua de la seguridad[1].

El dominio de Control de Accesos identifica en particular cuatro objetivos de control:

- Políticas de control de accesos
- Gestión de acceso de usuario
- Responsabilidades del usuario
- Control de acceso a sistemas y aplicaciones

[1] Sistema de Gestión de la Seguridad de la Información, SGSI, que define el estándar ISO/IEC 27001, pero del que no es objeto este proyecto.

Cada objetivo se podría decir que es la temática concreta en la que se agrupan los controles de seguridad y éstos tienen un efecto directo en una o varias de las dimensiones de seguridad habituales como la Confidencialidad, la Integridad, la Disponibilidad y la Trazabilidad.

Conocer cómo afecta a las dimensiones de la seguridad ofrece una idea de los riesgos que puede suponer para una organización el hecho de no aplicar los controles de seguridad indicados. Además, la tecnología ofrece ya multitud de herramientas y soluciones que favorecen la aplicación de los controles. Cuando una organización es grande, más que de control de accesos, se habla de gestión de identidades como un "todo" que gestiona, de manera organizada, la información sobre un usuario desde que entra en la organización siendo una persona con un nombre y apellidos determinados hasta cómo esa persona comienza a adoptar identidades en diferentes sistemas, aplicaciones o servicios, y cada uno con cuentas de usuario y características de permisos y privilegios adaptados a la propia persona.

A lo largo del proyecto, se analizarán cada uno de los controles de seguridad dispuestos por el estándar y se identificarán situaciones, características, buenas prácticas y herramientas que favorezcan su implantación. La identificación de métricas de seguridad asociadas a cada control para la creación de un cuadro de mandos será el punto y final del análisis.

Palabras clave: ISO/IEC 27002, seguridad de la información, estándar de seguridad, control de accesos, requisitos de seguridad de la información, confidencialidad, autenticación, autorización.

Abstract

This final project focuses on one of the domains that the version 2013 of the ISO/IEC 27002 standard manages. This domain is Access Control.

This standard defines a series of security objectives and controls associated with these objectives that consist on the minimum guidelines that any organization, regardless of its size, should apply. Although the application of specific security controls doesn't guarantee that 100% of attacks or security flaws are prevented, their application itself minimizes the appearance of them, especially when complemented with a continuous information security management model[2].

The Access Control domain identifies four control objectives:

- Access Control Policies
- User Access Management
- User Responsibilities
- Access control systems and applications

Each objective is related to the specific topic in which security controls are grouped and these have a direct effect on one or more of the usual security dimensions as confidentiality, integrity, availability and traceability.

[2] Information security management system, ISMS, as it is defined in the ISO/IEC 27001 standard. This standard is out of this project.

Knowing how it affects to security dimensions provides an idea of the risks they may pose to an organization the fact of doesn't apply the indicated security controls. In addition, the technology offers many tools and solutions that promote the implementation of controls. When an organization is large, more than access control, we talk about identity management as a "whole" that manages, in an organized manner, information about a user from entering the organization being a person with an specific name and surname to how that person begins to get different identities on systems, applications and services, each one with user accounts and permissions features and privileges tailored to the individual.

Throughout the project, it will analyze each of the security controls mandated by the standard and it will identify situations, features, best practices and tools that support their implementation. Identifying security metrics associated with each control for creating a scorecard will be an end to this analysis.

Keywords: ISO/IEC 27002, information security, security standard, access control, information security requirements, confidentiality, authentication, authorization.

Índice general

Índice de figuras

Índice de tablas

INTRODUCCIÓN AL PROYECTO Y OBJETIVOS

1. Introducción

Este proyecto fin de carrera se centra en uno de los dominios que trata la versión del 2013 del estándar ISO/IEC 27002 (ISO/IEC 27002, 2013).

Antes de introducir el sentido del proyecto, resulta interesante realizar un breve recorrido por la historia del propio estándar y presentar uno de los dominios de los que consta el estándar: el dominio de Control de Accesos, que es el dominio objeto de este proyecto.

1.1. Introducción al estándar ISO/IEC 27002

El estándar ISO/IEC 27002 es un estándar publicado por la International Organization for Standardization y la International Electrotechnical Commission.

La versión más reciente corresponde al año 2013 pero en realidad forma parte de un conjunto de estándares dedicados todos ellos a la seguridad de la información y que han conformado la llamada familia de estándares ISO/IEC 27000[3].

El estándar ISO/IEC 27002 es un estándar con recomendaciones y mejores prácticas en la gestión de seguridad de la información. Pero, no se cubren únicamente aspectos de seguridad de los sistemas de información desde una perspectiva únicamente de TI, sino que también se cubren aspectos organizativos entendidos como funciones de una organización que afectan a la seguridad de la información.

Los inicios de la norma se sitúan en la norma británica BS 7799 publicada en 1995, en concreto de su primera parte BS7799-1 (BS7799-1, 1995).

En el año 2000, la International Organization for Standardization y la International Electrotechnical Commission deciden adoptarla publicándola como ISO/IEC 17799 (ISO/IEC 17799, 2000) con el título "*Information technology - Security techniques - Code of practice for information security management*".

En el año 2005, la International Organization for Standardization y la International Electrotechnical Commission también adopta la segunda parte de la norma BS 7799 (BS7799-2, 1999), dedicada a la implementación de un sistema de gestión de la seguridad, que comúnmente se conoce por sus siglas SGSI. Publican la ISO/IEC 27001 (ISO/IEC 27001, 2005) con el título "*Information technology - Security techniques - Information security management systems - Requirements*" y es en ese momento en que

[3] La lista completa de estándares de la familia 27000, se puede ver en el Anexo de este documento.

dejan reservada toda la numeración 27000 para utilizarlos en los estándares para la Seguridad de la Información.

Ya en el año 2007, la norma ISO/IEC 17799 pasó a convertirse en la ISO/IEC 27002 y así integrarse en el marco de las normas 27000. La última revisión que se ha hecho de la norma tuvo lugar en el año 2013 y actualmente es la versión vigente.

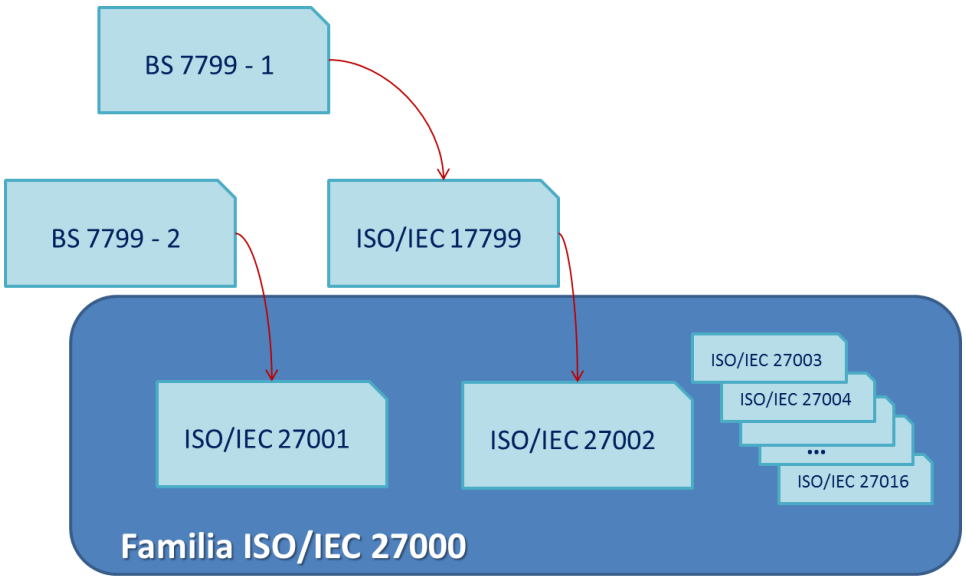


Figura 1. Evolución histórica del estándar ISO/IEC 27002 e ISO/IEC 27001

1.2. Introducción al dominio de Control de Accesos

La norma ISO/IEC 27002:2013 define un total de 114 controles generales de seguridad.

Estos controles de seguridad están estructurados u organizados en 14 dominios de seguridad. Uno de estos dominios es el referido al Control de Accesos.

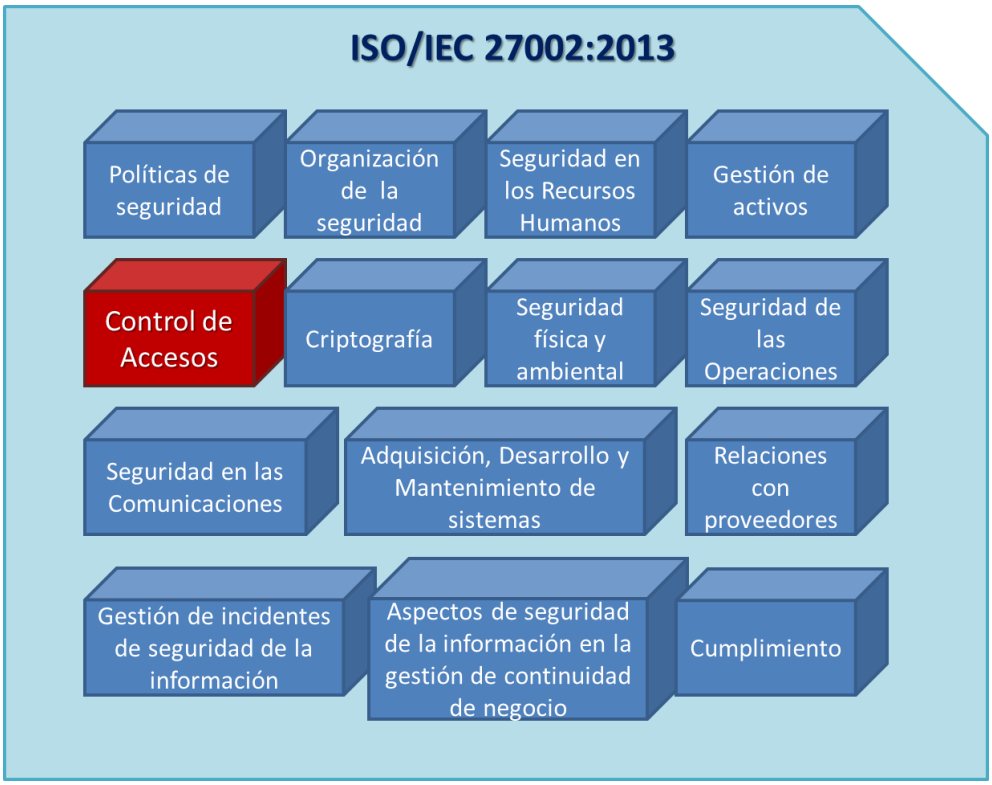


Figura 2. Dominios en los que se estructura ISO/IEC 27002:2013. Entre ellos el correspondiente a Control de Accesos

El estándar estructura los contenidos de cada dominio en lo que denomina *objetivos de control*. Y es dentro de cada objetivo de control donde se desarrollan cada uno de los controles de seguridad que el estándar recomienda.

El dominio de Control de Accesos en particular está estructurado en los siguientes cuatro objetivos de control:

1) Políticas de control de accesos
2) Gestión de acceso de usuario
3) Responsabilidades del usuario
4) Control de acceso a sistemas y aplicaciones

Estos cuatro objetivos, junto con los controles de los que constan, tratan de establecer un orden mínimo de actuaciones que puede ser exigible a cualquier organización:

- Se parte de la necesidad de existencia de una política de control de accesos, de alto nivel, que por un lado tenga en cuenta las necesidades de negocio para su definición y por otro sus requerimientos de seguridad. Este objetivo remarca el papel del "propietario" de los activos de información.

- El siguiente objetivo se centra en el control sobre el usuario, sobre sus mecanismos de identificación y de autenticación y en especial sobre sus permisos o privilegios.
- El tercer objetivo en cambio resalta el papel del "usuario" pero como colaborador imprescindible en el mantenimiento de la seguridad haciéndoles responsables de la aplicación y custodia de sus mecanismos de identificación y autenticación.
- Y su cuarto objetivo pone el foco de atención en la protección de los sistemas y aplicaciones, que al final son las herramientas con las que se trata la información.

Figura 3. Objetivos de control del dominio de Control de Accesos

1.3. Introducción al proyecto fin de carrera

Aunque el dominio de Control de Accesos en esencia puede resultar sencillo, su implantación en una u otra organización puede llegar a ser completamente diferente en función del tipo de organización de que se trate.

Además, una falta de control sobre cómo se está aplicando y la efectividad de sus medidas, puede hacer que lejos de favorecer el desarrollo de la actividad de la organización con efectividad y seguridad, se provoquen conflictos, brechas y discrepancias que terminen afectando a la organización, a la seguridad de su información y en definitiva poniendo en peligro su propio negocio.

Entender adecuadamente los controles de seguridad definidos, identificar los mecanismos técnicos y/u organizativos adecuados que los resuelven y definir indicadores que permitan a una organización valorar la adecuación de los mecanismos, es fundamental para que los controles resulten efectivos y perduren a lo largo del tiempo.

2. Objetivos del proyecto

El objetivo del proyecto es ofrecer maneras y puntos de vista sobre los controles de seguridad diferentes. Deberían permitir reflexionar a un hipotético Responsable de Seguridad de una organización cualquiera, sobre la mejor manera de implantar los controles de seguridad del estándar ISO/IEC 27002 (y en particular del dominio de Control de Accesos) en su organización.

Para ello, en el proyecto se realizará un estudio detallado de cada uno de los controles de seguridad identificados en la versión más reciente del estándar ISO/IEC 27002, la correspondiente al año 2013, y con ese estudio:

- Clarificar el objetivo y sentido de cada control.
- Identificar el impacto en las dimensiones de la seguridad de Confidencialidad, Integridad, Disponibilidad y Trazabilidad, que no aplicar el control puede suponer.
- Identificar buenas prácticas habituales y ejemplificar o destacar diferencias que puedan ser interesantes o peculiares según el tipo de organización.
- E identificar ejemplos de posibles herramientas o soluciones tecnológicas que puedan ayudar con el cumplimiento del control.

Pero, el análisis del dominio no sería completo si no se consideran también métricas sobre sus controles e indicadores que permitieran conocer el estado y situación de una posible implantación del dominio de la norma.

La frase "L*o que no se mide, no se puede mejorar. Lo que no se puede mejorar, se degrada*" [4] (Herce, 2012), a día de hoy sigue siendo más que vigente y su traslación a los Cuadros de Mando una realidad para muchas organizaciones y empresas.

La familia ISO/IEC 27000 también dedica uno de sus estándares a las métricas e indicadores para la gestión de la seguridad de la información, el estándar ISO/IEC 27004 (ISO/IEC 27004, 2013) por lo que también será un apoyo para la elaboración de este análisis.

[4] Según unos, frase de Lord Kelvin, siglo XVIII. Según otros, frase de Peter Drucker, mediados siglo XX)

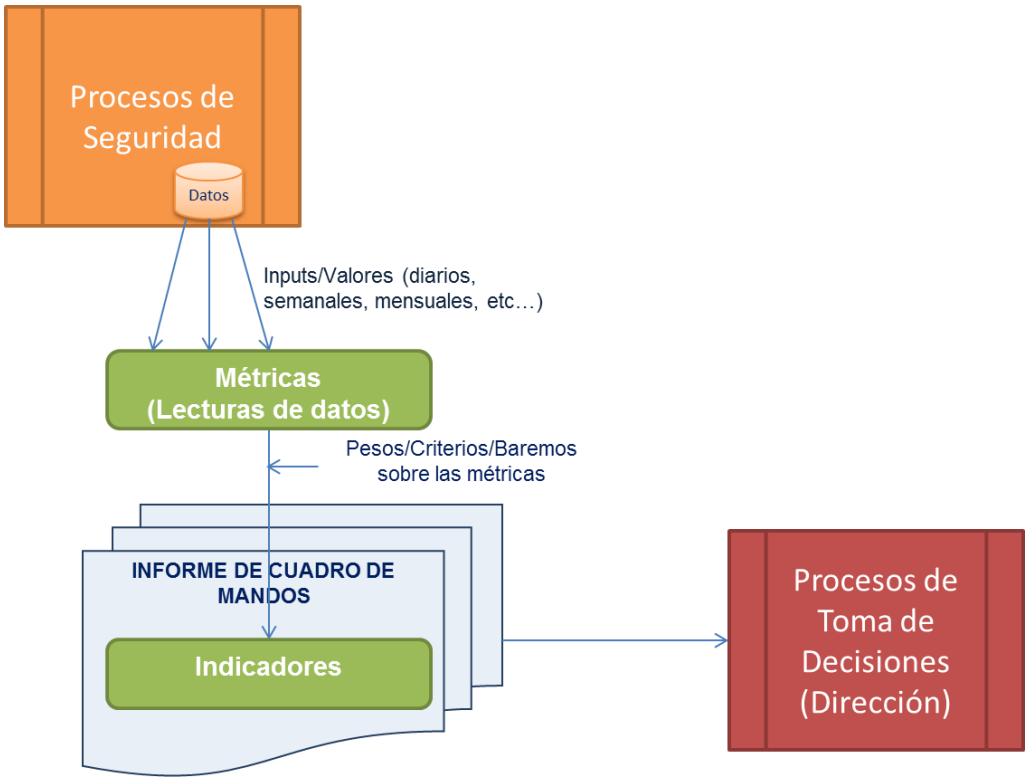


Figura 4. Funcionamiento simplificado de un cuadro de mandos

3. Fases del desarrollo y medios empleados

Este estudio ha sido realizado en aproximaciones por capas, hasta cubrir todos los aspectos tratados.

Inicialmente se trabajó en conocer, entender y traducir cada uno de los controles de seguridad descritos en el propio estándar y analizar cómo el hecho de tenerlo o no implantado podía afectar o impactar en aspectos como la Confidencialidad, la Integridad, la Disponibilidad y la Trazabilidad.

Una vez realizado para todos los controles y con el conocimiento más amplio sobre los controles, se realizaron subsiguientes pasadas sobre cada control identificando prácticas habituales que se realicen sobre el control en organizaciones que estuvieran en conocimiento del autor de este documento para así compararlo con recomendaciones y buenas prácticas habituales de mercado. El conocimiento y experiencia en diferentes empresas del autor de este documento, junto con el uso de internet para la búsqueda de recomendaciones, políticas de seguridad de organizaciones que pudieran estar publicadas así como la identificación de herramientas y análisis de sus capacidades de configuración, son las que han permitido aportar las recomendaciones y reflexiones expuestas en este proyecto.

A continuación se recogen las referencias a algunas de estas páginas:

- (ISO - The International Organization for Standardization)
- (Portal de ISO 27002)
- (ISO 27001 e ISO 27002: Dominio 11 - Control del Acceso)
- (Blog Seguridad de la Información)
- (ISO 27001 e ISO 27002)
- (Noticias sobre Seguridad de la Información)
- (Cumplimiento seguridad y control en la nube es posible)
- (Critical Security Controls)

La última fase ya fue dedicada a la identificación de posibles objetivos interesantes de medir relacionados con el control para así identificar sus métricas. Será la base para el ejemplo de cuadro de mandos elaborado como colofón de este proyecto.

Estas son algunas referencias a fuentes de soporte utilizadas para este contexto del documento:

- (Norma 27004, 2014)
- (ISO/IEC 27004 – Medición de la Seguridad de la Información, 2014)

- (10 identity management metrics that matter, 2011)
- (ISO 27001 e ISO 27004)
- (Security metrics and the balanced scorecard, 2011)
- (Gestión con Indicadores. Cuadro de mando, 2011)

4. Estructura del documento

Para facilitar la lectura de la memoria, se incluye a continuación un breve resumen de la estructura y contenidos de este documento:

- **Sección 1**: Introducción y Objetivos

  Corresponde al presente módulo y sus capítulos pretenden describir el sentido e intenciones del proyecto antes de entrar en sus detalles, así como los medios para realizarlo.

- **Sección 2**: Dominio de seguridad: Control de Accesos

  La segunda sección del documento es el centro del proyecto. Se compone de cuatro capítulos, uno para cada uno de los cuatro objetivos de control que define el dominio de Control de Accesos.

  Para cada objetivo de control, el proyecto se adentrará en cada uno de los **controles de seguridad** de los que el estándar indica que se compone el objetivo y de ellos se realizará un estudio estructurado de la siguiente manera:

  #### Definición ISO

  Traducción del control de la norma. Es una traducción libre realizada por el autor de este proyecto.

  #### Guía de implementación ISO

  Traducción libre realizada por el autor de este proyecto. En ocasiones es una versión abreviada de las recomendaciones de implementación que proporciona la norma, destacando aquellas más importantes.

  #### Riesgos de seguridad

  Riesgos en los que se puede incurrir por no tener implementado el control. Se analizarán principalmente las implicaciones que pueda tener en los siguientes cuatro objetivos básicos de la seguridad:

  - ✓ **Confidencialidad** → consiste en poder garantizar que la información sólo es accesible a aquellas personas autorizadas a ello.
  - ✓ **Integridad** → consiste en poder garantizar que la información no puede ser alterada por personas no autorizadas.
  - ✓ **Disponibilidad** → consisten en poder garantizar que la información estará accesibles siempre que se necesite.

- ✓ **Trazabilidad** → consiste en poder garantizar que se puede relacionar cualquier acción realizada sobre un recurso con el usuario, aplicación, sistema, dispositivo o proceso que la realizó y el momento concreto en que tuvo lugar.

Se descarta contemplar otros objetivos habituales de la seguridad como son la **Autenticación** y la **Autorización**, por dos motivos:

1. Se les puede considerar una derivada del objetivo de la confidencialidad. La autenticación y la autorización son objetivos habituales en muchas referencias bibliográficos, aunque a veces son tratados como objetivos de la seguridad y otras como servicios de la seguridad. Precisamente cuando son considerados servicios, se convierten claramente en una derivada por tanto de los objetivos de seguridad y a efectos de este proyecto se van a considerar como tal.
2. El objetivo del proyecto se centra en el dominio de Control de Accesos que en definitiva es la existencia de autenticación y autorización. En su análisis no tiene sentido que uno de los objetivos de seguridad contra los que se analizará cada control del dominio sea en sí mismo la definición del propio dominio.

Recomendaciones y Buenas prácticas

En este apartado se proporcionarán recomendaciones y buenas prácticas resultado de analizar y comparar prácticas aplicadas en diferentes organizaciones y buenas prácticas habituales de mercado. Proporcionará ideas, reflexiones y recomendaciones interesantes atendiendo a diferentes casuísticas y tipos de organización.

Tecnologías aplicables

Se identificarán tecnologías que puedan ayudar o favorecer el cumplimiento del control, puesto que en muchos casos existen tecnologías y productos específicos que resuelven sobre ciertos controles.

Métricas para el cuadro de mando

Y por último, sobre cada control se identificará un conjunto de métricas e indicadores interesantes para medir el grado de implantación y cumplimiento de cada uno de los controles del estándar.

- **Sección 3**: Cuadro de Mandos.

  La tercera sección del documento mostrará un ejemplo de cuadro de mandos sobre el cumplimiento del dominio de Control de Accesos para una hipotética Gerencia o Dirección de una organización, utilizando algunas de las métricas identificadas a lo

largo del proyecto. La presentación y diseño de los indicadores se adecuará a lo recogido en el estándar ISO/IEC 27004.

- **Sección 4**: Conclusiones

  Recogerá las conclusiones finales tras la elaboración del proyecto fin de carrera.

- **Sección 5**: Presupuesto y Planificación

  Esta sección contendrá el presupuesto detallado y planificación para la elaboración del proyecto.

- **Sección 6**: Anexos

  Y para finalizar se recogerán en la última sección del documento a modo de anexos, la familia ISO/IEC 27000, el glosario y la bibliografía y referencias utilizadas a lo largo de la elaboración del proyecto.

DOMINIO DE SEGURIDAD: CONTROL DE ACCESOS

1. Requisitos de negocio para el control de accesos

ISO/IEC 27002 establece como objetivo de los requisitos de negocio para el control de accesos el que se limite el acceso a la información así como a las herramientas con las que se procesa.

Bajo este objetivo, la norma establece dos controles que se analizarán a continuación:

1. Política de control de accesos
2. Acceso a redes y servicios de red

1.1 Política de control de accesos

1.1.1 Definición ISO

Se debe establecer, documentar y revisar una política de control de accesos en base a los requisitos o necesidades de negocio y de seguridad.

1.1.2 Guía de implementación ISO

Se deben establecer de forma clara en la política de control de acceso reglas, derechos de acceso y restricciones de acceso por roles de usuarios y los usuarios y/o proveedores de servicios deben estar informados de las políticas de control de acceso que deben cumplir.

Son cada uno de los propietarios de los activos, en función de los riesgos de seguridad de la información, quienes establezcan los controles de acceso necesarios para su activo. Implican acceso lógico pero también acceso físico.

La política debería recoger o tener en cuenta los siguientes aspectos:

- Requisitos de seguridad para cada aplicación de negocio.
- Políticas para la distribución (diseminación) de información y de autorización de acceso a ésta.
- Consistencia entre los derechos de acceso otorgados y las políticas de clasificación de la información de sistemas y redes.

- Legislación relevante que sea aplicable o cualquier otra obligación contractual que pueda limitar acceso a datos o servicios.
- La gestión de derechos de acceso para entornos en red y distribuidos, contemplando todos los posibles tipos de conexión que tenga disponibles.
- Segregación de los roles de control de acceso, por ejemplo, diferenciando entre solicitudes de acceso, autorización de accesos y administración de accesos.
- Requisitos para autorizar formalmente una solicitud de acceso.
- Requisitos para realizar revisiones periódicas de los derechos de acceso.
- Eliminación de derechos de acceso.
- Almacenamiento de registros de todo evento significativo relacionado con el uso y la gestión de las identidades de los usuarios así como de su información secreta de autenticación.
- Los roles con accesos privilegiados.

La norma además recuerda algunas estrategias interesantes que pueden aplicar las organizaciones y tomar en consideraciones:

- Establecer el control de acceso utilizando la premisa de que “por defecto, todo está prohibido, salvo lo que esté expresamente permitido” mejor que la premisa de que “todo está permitido salvo lo que esté expresamente prohibido”.
- Los principios para otorgar acceso a la información suelen ser “la necesidad de saber” y “la necesidad de utilizar”.
- Las reglas de control de acceso deben estar sustentadas por procedimientos formales que las definan y por las responsabilidades de los usuarios. Materializarlo en roles suele ser una manera exitosa de que las organizaciones trasladen los derechos de acceso a roles de negocio y con ellos hasta los usuarios.

La norma también recuerda algunas precauciones que se deben tener:

- Con los cambios de etiquetado o clasificación de información, cuando puedan ser iniciados automáticamente mediante el uso de utilidades de tratamiento de datos que un usuario pueda utilizar de manera discrecional.
- Con los cambios en permisos de usuarios que puedan ser iniciados automáticamente desde algún sistema de información que pueda utilizar un administrador de manera discrecional.
- Con las reglas que requieren aprobación expresa antes de otorgarlas frente a reglas que no lo requieren.

1.1.3 Riesgos de seguridad

El hecho de que una organización no tenga una política de control de acceso significa que no se tiene por qué aplicar ningún criterio “ordenado” que restrinja u otorgue acceso a la información. Por ejemplo, el propietario de cada aplicación decidiría por sí mismo quién o quiénes pueden acceder y esa decisión no estaría basada en coherencia con aspectos organizacionales, sino puramente personales.

Tener una política de control de acceso, que no sea clara, también es un problema, puesto que puede provocar contradicciones a la hora de autorizar un determinado nivel de acceso. Por ejemplo, podría ocurrir que a un usuario no se le otorgue acceso a una información desde un determinado sistema A, pero en cambio sí lo consiga por tener acceso desde un sistema B.

Por tanto, no tener una política de control de accesos o que no sea clara supone un riesgo importante sobre la confidencialidad de la información en primer lugar, pero también sobre los restantes objetivos de seguridad (integridad, disponibilidad y trazabilidad).

1.1.4 Recomendaciones y Buenas prácticas

Dado el tipo de información que una política de control de accesos puede recoger, puede llegar a convertirse en un documento excesivamente técnico y además con cierta volatilidad por los cambios normales que puede sufrir una organización, más habitual cuanto más grande sea una organización: aplicaciones nuevas, aplicaciones que desaparecen, reorganización de personal, de la dirección, cambios de segmentación, etc.

La mejor manera de garantizar la usabilidad, coherencia y validez de una política de control de acceso es que ésta se organice en varios documentos jerárquicos, es decir, se inicie la política de control de accesos primero en un documento de alto nivel, que además sea promovido por la Dirección de la organización y que estipule la exigencia de controles de acceso, sus características, la responsabilidad sobre los controles de acceso y las pautas generales a aplicar. Es importante resaltar que una política de control de accesos debe aplicar a toda la organización. Nunca deben quedar excluidos ni personas, ni departamentos, ni sistemas.

La existencia de una política de control de accesos de alto nivel promovida por la Dirección de una organización, lo cual permite demostrar el compromiso de ésta con su cumplimiento y garantizar el alineamiento con los requisitos de negocio. Además, por tratarse de requisitos de alto nivel, su validez puede perdurar a lo largo del tiempo.

Tras la política de control de accesos de alto nivel, ya se podrán derivar N políticas de control de accesos dedicadas específicas por áreas, por aplicaciones, por líneas de negocio o por cualquier otro criterio de tal manera que este segundo nivel pueda estar mucho más cerca de la realidad tecnológica y así precisar y especificar cuanto se necesite de manera detallada. Este tipo de políticas de control de acceso de más bajo

nivel son más susceptibles de verse modificadas a los largo del tiempo, pero al tener un alcance más concreto, la gestión de estos cambios es adecuada y además, como estaría supeditada al cumplimiento con la política de alto nivel, la coherencia en los controles de acceso dentro de una organización será mantenida.

En función del tamaño de la organización, la forma de definir quiénes y cómo pueden acceder a qué aplicaciones o sistemas, puede derivar en un proceso sencillo o verdaderamente complicado:

- En organizaciones pequeñas, lo más probable es que la definición se realice aplicación por aplicación y se identifique cada usuario con los permisos o privilegios concretos que le corresponden. Al tratarse de una organización pequeña, el volumen de aplicaciones será habitualmente relativamente pequeño y un control tan directo es aceptable.
- Cuando el tamaño de la organización aumenta, la asignación de accesos de esta manera tan directa, deja de ser efectiva y sobre todo sostenible a lo largo de tiempo. El esfuerzo de inventariar sistemas y de inventariar sus usuarios es alto y cuando el volumen es grande, también se hace grande la probabilidad de que la información se quede obsoleta en poco tiempo. Por tanto, según aumenta el tamaño de una organización, la definición de la política de control de accesos debe realizarse en base a reglas que:
    - Por un lado generalicen o tipifiquen los tipos de aplicaciones, por ejemplo en base al nivel de exposición a internet, a la criticidad de la aplicación respecto de clientes, a la clasificación del tipo de dato gestionado, a la necesidad de cumplimientos legales de unas u otras aplicaciones, etc.
    - Y por otro lado tipifiquen los tipos de usuarios existentes en la aplicación. Tradicionalmente la tipificación de usuarios siempre se realizó en base a *Grupos de Usuarios* pero cada vez más se va sustituyendo por un modelo y nomenclaturas más cercanas al negocio, los llamados *Roles* o *Perfiles* de usuarios.

Lo que es importante en cualquiera de los casos, es que periódicamente se realice una revisión de la política que analice la viabilidad y todavía vigencia de ésta.

1.1.5 Tecnologías aplicables

La existencia de una política es un control organizativo, no técnico, tiene carácter documental, de definición de estrategia, por lo que no hay herramienta, tecnología o solución que directamente facilite el desarrollo e implantación de este control.

Lo que sí existen son herramientas y soluciones que permiten medir el grado de implantación de la política en los sistemas y aplicaciones. Son las llamadas ***soluciones de control de cumplimiento***. Si este tipo de herramientas se utiliza de manera periódica, entonces se podrán medir dos factores:

- El grado de penetración que la política de control de accesos tiene en los sistemas de información de una organización.
- El grado de degradación de los controles exigidos por la política a lo largo del tiempo.

Un ejemplo de una herramienta comercial de este tipo es Symantec Control Compliance Suite[5] .

Pero, en lugar de herramientas, puede aplicarse un proceso de auditoría. En este caso, existiría un equipo de personas, que en posesión de la política de control de accesos y un inventario de los sistemas, audite periódicamente el cumplimiento de la misma.

1.1.6 Métricas para el cuadro de mando

Algunas preguntas interesantes para verificar el grado de cumplimiento de este control serían:

- ✓ ¿Existe una política definida y escrita que estipule cómo y de qué forma se puede acceder a las aplicaciones y sistemas de la organización?
- ✓ ¿Se revisa periódicamente esta política?
- ✓ ¿Existen aplicaciones de negocio que no se vean afectadas por esta política, es decir, que queden fuera del ámbito de aplicación de la política? ¿cuántas (%), con respecto al número total de aplicaciones de negocio existentes en la organización?
- ✓ ¿En cuántos sistemas ya se ha implantado la política? ¿qué porcentaje representa respecto del total de los sistemas alcanzados por la política?
- ✓ ¿Cuántas deficiencias o no cumplimientos se han identificado en un período de revisión (para un sistema en concreto, o para un área o departamento, o para la organización en su totalidad? ¿ha aumentado o disminuido respecto a no cumplimientos obtenidos de revisiones anteriores?

Cuanto mayor sea el porcentaje de aplicación de la política en las aplicaciones, significará que mayor es la penetración de la política de control de accesos.

Y si el grado de penetración de la política es algo, cuanto menor sea el número de deficiencias identificadas, será un indicador del nivel de madurez de la organización respecto a las políticas de control de accesos.

[5] http://www.symantec.com/control-compliance-suite/

1.2 Acceso a redes y a servicios de red

1.2.1 Definición ISO

Los usuarios sólo deben tener acceso a las redes y servicios de red para los que hayan sido específicamente autorizados.

1.2.2 Guía de implementación ISO

Se debe definir una política para el uso de la red y de sus servicios que además sea consistente con respecto a la política de control de accesos[6] que se hubiera definido en la organización.

La norma recomienda que la política de acceso a redes y servicios de red incluya:

- Las redes y servicios de red a los que está permitido que se acceda.
- Los procedimientos de autorización de acceso.
- Los controles y procedimientos de gestión que protegen el acceso a las conexiones y servicios de red.
- Los mecanismos utilizados para acceder a las redes y sus servicios (por ejemplo, el uso de VPN o de redes inalámbricas).
- Requisitos para la autenticación de usuarios en su acceso a los servicios de red.
- Monitorización del uso de los servicios de red.

1.2.3 Riesgos de seguridad

El hecho de tener acceso a redes y servicios de red para los que no tuviera autorización expresa genera un riesgo sobre la confidencialidad de la información y también sobre la integridad y disponibilidad de la misma.

La no utilización de una política que lo gestione, puede llegar a provocar contradicciones a la hora de autorizar un determinado acceso así como generar riesgos en los controles de seguridad establecidos a nivel de aplicación, por ejemplo. De nuevo, se generan directamente riesgos sobre la confidencialidad, la integridad y la disponibilidad de la información.

[6] Ver apartado "*1.1Política de control de accesos*" de este documento.

1.2.4 Recomendaciones y Buenas prácticas

La realidad actual de toda organización es cada vez más todo está expuesto al exterior, a Internet.

Las formas de acceso a los servicios, aplicaciones de negocio e información que una organización debe contemplar cada vez son más variopintas. Ya no sólo el acceso se realiza desde PCs o portátiles, sino que se deben contemplar la variedad de dispositivos móviles hoy en día imprescindibles como son los smartphones, las tablets, o los netbooks.

El uso de estos medios de acceso a los servicios, sistemas e información interna de una organización, ha generado la necesidad de contemplar al menos tres tipos de accesos atendiendo al tipo de conexión y con ello la necesidad de una política específica para cada uno de ellos:

- Acceso desde las redes internas de la organización, por cable.
- Acceso desde redes WIFI corporativas.
- Acceso desde redes externas a la organización, entre las que se pueden enumerar: la red de casa del empleado, WIFIs públicas, cibercafés, etc. Este tipo de acceso quedan fuera del control de la organización, lo que provoca que se tengan que reforzar otras medidas de control de acceso.

Este escenario hace más que recomendable que toda política de acceso a redes contemple dos requisitos:

- Exigencia de una adecuada segregación o segmentación de redes, lo que facilitará aplicar controles de acceso de uno a otro segmento.
- Necesidad de despliegue de soluciones para el acceso seguro desde el exterior a los usuarios de una organización, generalmente mediante soluciones de VPN.

1.2.5 Tecnologías aplicables

De la misma manera que en el control anterior, este control es de índole organizativo, es documental, de estrategia y no técnico, por lo que no aplica hablar de herramientas, tecnologías o soluciones que directamente colaboren en la implantación de este control.

1.2.6 Métricas para el cuadro de mando

Algunas preguntas interesantes para verificar el grado de cumplimiento de este control serían:

- ✓ ¿Existe una política definida y escrita que estipule cómo y de qué forma se puede acceder a las redes y servicios de la organización?
- ✓ ¿Contempla la política la existencia de una segmentación de redes y define quiénes pueden tener acceso a cada segmento?
- ✓ ¿Contempla la política diferenciar entre los diferentes medios de acceso y establece controles sobre ellos?
- ✓ ¿Se revisa periódicamente esta política?

Cuanto más exhaustiva sea la definición de la política, mayor será el grado de madurez de la organización respecto al control de accesos.

2. Gestión de acceso de usuarios

ISO/IEC 27002:2013 establece como objetivo de la gestión de acceso de usuarios el asegurar que el acceso de los usuarios está autorizado y que se prevengan los accesos no autorizados a sistemas y servicios.

2.1 Registro y des-registro de usuarios

2.1.1 Definición ISO

Debe existir un proceso formal para registrar y des-registrar usuarios que permita después otorgar o revocar derechos de acceso.

2.1.2 Guía de implementación ISO

El proceso para gestionar los identificadores de usuarios debería incluir:

- La utilización de identificadores de usuario unívocos, de tal manera que siempre se pueda identificar a la persona física a la que pertenece y que se pueda por tanto responsabilizar de las acciones realizadas con él. La utilización de identificadores compartidos sólo debe estar permitida cuando sea necesario por motivos operativos o de negocio y en dichos casos será aprobado y debidamente documentado.
- El bloqueo o eliminación inmediata de identificadores de usuarios que abandonen la organización.
- La comprobación periódica, y la eliminación o el bloqueo de aquellos identificadores de usuario que sean redundantes.
- La garantía de que no se entregan identificadores de usuario redundantes a otros usuarios.

En general, el proceso de otorgar o revocar acceso a la información o a las herramientas que lo procesas suelen realizarse en dos pasos:

- Primero asignar/activar (o revocar) un identificador de usuario.
- Después proveer (o revocar) derechos de acceso a su identificador de usuario.

2.1.3 Riesgos de seguridad

El principal riesgo para una organización cuando no posee un proceso formal de registro (y des-registro) de usuarios es que pierde la posibilidad de identificar las acciones realizadas por cada usuario, perdiendo toda trazabilidad.

Si una organización utiliza procesos formales de registro de usuarios, pero no existe homogeneidad entre los identificadores de usuario o de cuentas utilizados entre las diferentes aplicaciones, obtiene una trazabilidad local a cada aplicación, pero pierde la posibilidad de trazabilidad global y le imposibilita por tanto a conocer el alcance total de las acciones realizadas por un usuario.

2.1.4 Recomendaciones y Buenas prácticas

Aunque el control está centrado en el registro (y des-registro) del usuario, en la práctica este proceso siempre se realiza junto a la solicitud propia de acceso, bajo determinados perfiles, permisos o privilegios en el sistema. Contemplar ambos procesos por separado permite centrarse en el instante de creación y asignación de un identificador de usuario o identificador de cuenta para el usuario solicitante.

El uso de identificadores unívocos y no compartidos en cada aplicación, como recomienda el estándar es un concepto importante y aunque puede parecer sencilla la idea de asignar un identificador, que sea de uso personal y que siempre sea diferente a cada usuario, en la práctica no es tan sencillo por varios motivos:

a) Por la naturaleza de la Organización.

   Existen infinidad de modelos de funcionamiento de las Organizaciones, pero hay uno en particular, en el que el uso de identificadores unívocos y personales particular es especialmente complejo.

   Se trata de las Organizaciones con departamentos en los que la rotación de personal es muy alta, como suelen ser los departamentos de HelpDesk o departamentos de Atención al Cliente, al Empleado, etc:

   - Este tipo de departamentos requieren de aplicaciones y sistemas que suelen están muy granuladas en cuanto a permisos de acceso.
   - Además, cuando entra un nuevo empleado la necesidad de agilidad en obtener los accesos es primordial, lo que implica que necesita rápidamente un identificador de usuario y rápidamente acceso a todas las aplicaciones necesarias con la complejidad de permisos que esos departamentos suelen llevar implícitos.

   La solución que suelen adoptar este tipo de departamentos es hacer pre-existir un pool o conjunto de cuentas de usuarios con las variantes de permisos que

necesitan. Los responsables del departamento se encargan de llevar, manualmente, una lista que asocia qué usuario tiene cada empleado en el momento. Cuando un empleado sale de la Organización, no se des-registra el identificador, sino que se le des-asigna de la persona que lo utilizaba. Así queda disponible para futuros empleados.

Es recomendable en estos casos aplicar las siguientes medidas de seguridad, en el instante de la salida del empleado:

- Cambiar inmediatamente la contraseña de acceso del identificador de usuario que utilizaba (evitando así posibles usos fraudulentos).
- Bloquear por un período de tiempo suficientemente amplio el identificador de usuario con objeto de facilitar posibles investigaciones de trazabilidad en el corto plazo. Finalmente los identificadores sí son reutilizados por diferentes empleados, por lo que si la pertenencia de un usuario de una persona a otra es inmediata y se ve afectado por una investigación, la utilización en activo del identificador podría dificultar investigaciones.

b) Por el propio volumen de aplicaciones diferentes existentes.

En Organizaciones grandes, el volumen de sistemas y aplicaciones es también grande. Aunque la Organización decida exigir en su política de control de accesos que todos los empleados deben tener un identificador de usuario personal y unívoco, en la práctica puede ocurrir que el formato o nomenclatura que se decida utilizar no se pueda aplicar en todas las aplicaciones.

Contra más grande sea una Organización, más frecuente es ya que hablen de Gestión de Identidades y no de Gestión de Usuarios. Los **Sistemas de Gestión de Identidades, IdM**, también son conocidos como **IAM (Identity and Access Management)**.

Por *Identidad de usuario* se puede entender una ficha personal de un empleado, es decir, el conjunto de su nombre, apellidos, otros datos personales y el dato más importante: un identificador de usuario corporativo o código de empleado, o número de empleado… Este identificador puede adoptar en las Organizaciones diferentes nombres, pero constituye un código identificativo del usuario a lo largo de la Organización.

Una *Cuenta de usuario*, en cambio, es cada una de las mini-fichas que un empleado tiene en cada una de las aplicaciones y sistemas a los que requiere acceso. Las aplicaciones ya no requieren guardar más datos del usuario que no sea su identificador de usuario.

Con estos dos conceptos, la Gestión de Identidades lo que define es que un empleado es en realidad una “identidad” que tiene múltiples cuentas de usuario (una cuenta por cada sistema o aplicación sobre la que necesita acceso).

Las aplicaciones de Gestión de Identidades precisamente son las que se encargan de guardar la relación entre la Identidad de un empleado y todas sus cuentas de usuario. En general centralizan la creación de las identidades y se alimentan de cada nueva cuenta que se abre a un usuario. Este control es el que permite:

- Garantizar la trazabilidad de las acciones realizadas por un usuario en Organización, de manera global, aunque se utilicen identificadores diferentes para las cuentas de un usuario.
- Y también muy importante el hecho de facilitar que cuando, por ejemplo un empleado se va, pueda asegurarse que se le cierran todas sus cuentas de usuario, y cuando así ha sido, se cierra o bloquea su identidad, es decir, garantiza el des-registro de los usuarios.

Por último, remarcar que el uso de nomenclaturas de usuario homogéneas entre las diferentes aplicaciones, sistemas o recursos de una Organización, además de facilitar que una Organización tenga trazabilidad de todas las acciones que realiza un usuario en su Organización de forma más sencilla, también permite, con ayuda de sistemas expertos de correlación de eventos de seguridad, la posible detección anticipada de acciones fraudulentas por parte de sus usuarios o empleados.

Este tipo de sistemas se les conoce como sistemas **SIEM (Security Information and Event Management)** y su funcionamiento está basado en la búsqueda de patrones de acciones realizadas por los usuarios dentro de los logs de las aplicaciones. Cuando localiza patrones de ciertas conductas o eventos en un log, aplica reglas de relación para tratar de detectar ataques de seguridad o violaciones de las políticas de seguridad. Por ejemplo:

- Se detecta en el log de un servidor que se han producido intentos de autenticación fallidos repetidos desde una cierta IP con un cierto identificador de usuario.
- En el log del ldap corporativo, en cambio se puede apreciar un cambio de permisos del usuario con el que casualmente se están produciendo los intentos de autenticación fallidos y dichos cambios de permisos le han convertido en administrador.

Por separado, estos dos logs sería probable que no llamaran la atención de ningún administrador de los sistemas, pero relacionados, sí podrían ser una señal de, por ejemplo, un intento de ataque por fuerza bruta con un usuario al que ya han conseguido proporcionarle permisos de administración.

2.1.5 Tecnologías aplicables

Desde el punto de vista del proceso de Registro y Des-registro que exige el estándar, existen multitud de aplicaciones de gestión de peticiones. Entre las más potentes y

conocidas de pago, se encuentra Remedy[7] y en el entorno del software libre, Request Tracker, RT[8].

En cambio, si asociamos el proceso de Registro y Des-registro a la complementaria acción de solicitud de permisos de acceso, además de poder gestionarlo desde las herramientas antes mencionadas, también se tienen que contemplar las herramientas expertas en Gestión de Identidades, de las que hay multitud de productos como IBM Security Identity Manager[9] o NetIQ Identity Manager[10].

2.1.6 Métricas para el cuadro de mando

Algunas preguntas interesantes para verificar el grado de cumplimiento de este control serían:

- ✓ ¿Existe un proceso formal para solicitar el registro y des-registro en la Organización?
- ✓ ¿Existe una aplicación o herramienta en la que se gestionen automáticamente las peticiones de registro y des-registro?
- ✓ ¿Cuántas aplicaciones y sistemas disponen de un proceso formal para el registro y el des-registro y que utilizan la herramienta de peticiones? ¿Qué porcentaje supone respecto del total existente en la organización?
- ✓ ¿Cuántas aplicaciones y sistemas disponen de un proceso formal para el registro y el des-registro, pero que no utilizan la herramienta de peticiones? ¿Qué porcentaje supone respecto del total existente en la organización?
- ✓ ¿cuántas aplicaciones y sistemas no disponen de ningún proceso formal y por tanto quedan fuera del control de la organización?

Cuando existe herramienta automática para la gestión de peticiones, además es interesante identificar la siguiente información, por ejemplo para evaluar mensualmente:

- ✓ ¿Cuántas peticiones son de registro y cuántas de des-registro?
- ✓ ¿Cuál es el tiempo medio de resolución de una petición de registro o des-registro?
- ✓ ¿Cuántas peticiones están en espera de ser validadas en un instante determinado y cuánto tiempo llevan esperando?

La información más importante que proporcionan estas métricas es en primero lugar el nivel de formalidad que existe en una organización. Si ni siquiera para el registro y des-

[7] http://www.bmcsoftware.es/it-solutions/remedy-itsm.html

[8] https://www.bestpractical.com/rt/

[9] http://www-03.ibm.com/software/products/es/identity-manager

[10] https://www.netiq.com/es-es/products/identity-manager/advanced/

registro existe un proceso, poca fiabilidad puede producir cualquier control posterior que trate de controlar la asignación de privilegios.

Por otro lado, las métricas respecto a los tiempos medios para resolver una petición. Aunque los tiempos para registro pueden ser un indicativo de eficiencia, desde el punto de vista de la seguridad lo que será importante será el tiempo medio para resolver una petición de des-registro. Tardar mucho en resolverlo significa que existe un usuario activo en algún sitio que no debería ya estarlo, por lo que se trata de un riesgo de seguridad para una organización.

Y por último, las métricas que evalúan el volumen de peticiones de alta o de baja. Cuando sus resultados se cruzan con las cursadas por Recursos Humanos de una organización, se ofrecen indicadores muy interesantes:

- En lo que respecta al volumen de altas, si no coincide, indica que los procesos de aprovisionamiento son ineficientes.
- En lo que respecto al volumen de bajar, si no coincide, da una referencia del volumen de cuentas de usuario obsoletas que puede tener una organización. Las cuentas de usuario obsoletas pueden convertirse en un punto débil de alto riesgo.

2.2 Aprovisionamiento del acceso de usuarios

2.2.1 Definición ISO

Debe existir un proceso formal de aprovisionamiento de accesos de usuarios para otorgar o revocar derechos de acceso a todo tipo de usuarios sobre todos los sistemas y servicios.

2.2.2 Guía de implementación ISO

El proceso de aprovisionamiento para otorgar o revocar derechos de acceso a identificadores de usuario debería incluir:

- La obtención de autorización por parte del propietario del sistema de información o del servicio para el uso del sistema de información o del servicio; también sería apropiado la obtención de una aprobación diferente de los derechos de acceso por parte de los responsables o gestores de los usuarios.

- Verificación de que el nivel de acceso otorgado es apropiado respecto a las políticas de acceso[11] y consistente con otros requisitos como los de segregación de tareas.

En general, el proceso de otorgar o revocar acceso a la información o a las herramientas que lo procesas suelen realizarse en dos pasos:

- Primero asignar/activar o revocar un identificador de usuario.
- Después proveer o revocar derechos de acceso a su identificador de usuario.

2.2.3 Riesgos de seguridad

La carencia de procesos formales de aprovisionamiento de usuarios puede provocar el otorgar de manera no controlada ni coherente permisos de acceso sin que además esté en conocimiento de los propietarios de la información, es decir, sin su autorización.

Esto implica un riesgo directo contra la confidencialidad, integridad y disponibilidad de la información.

2.2.4 Recomendaciones y Buenas prácticas

No cabe duda de la importancia de la existencia de un proceso formal para solicitar acceso a un sistema, aplicación o información. Pero además de existir el proceso, es importante que éste cuente también con mecanismos de seguridad durante su ejecución.

En general, un proceso de solicitud de acceso a un sistema, suele consistir de los siguientes pasos:

- Envío de solicitud (petición)
- Validación de petición para su aprobación o denegación
- Resolución/ejecución de la petición

En cada uno de estos pasos pueden hacerse consideraciones de seguridad interesantes de contemplar:

- ENVÍO DE SOLICITUD

  Sea cual sea el mecanismo utilizado para enviar una solicitud, es importante que en destino siempre sean almacenadas todas las solicitudes de acceso recibidas, con objeto de poder ser consultadas en el futuro en caso de incidencias o problemas.

[11] Ver apartado "*1.1Política de control de accesos*" de este documento.

Además, de almacenarse, siempre debería estar disponible la posibilidad de poder consultar en cualquier momento el estado o situación en que se encuentra una solicitud, al menos distinguiendo entre Recibida pero pendiente de validación y/o implantación, Aprobada e implantada o por último Rechazada y notificado al solicitante.

- VALIDACIÓN/AUTORIZACIÓN DE PETICIÓN

  Un proceso de validación de una solicitud de acceso, requiere que el validador conozca perfectamente quién quiere acceder (es decir, el usuario), a qué quiere acceder (es decir, el sistema, aplicación o información objetivo de la solicitud) y para qué (es decir, los permisos que requiere).

  El papel del "responsable del activo" que el primer control de seguridad resaltaba, cobra aquí todo su sentido. El responsable del activo es la mejor persona que puede resolver sobre si un solicitante puede o no acceder, puesto que es el mejor conocedor del sistema, aplicación o información que va a ser accedida y a quién un uso o acceso fraudulento más impacta.

- RESOLUCIÓN/EJECUCIÓN DE PETICIÓN

  Una vez aprobada o denegada una solicitud de acceso, también debe garantizarse la trazabilidad sobre quién ejecutó finalmente la petición en el sistema o aplicación de destino, a qué cuenta de usuario se lo otorgó y con qué privilegios. Para este aspecto, el estándar de seguridad dedica parte de sus controles, como se verá más adelante, en el apartado dedicado a la utilización de programas o utilidades privilegiadas[12].

  Por último, es frecuente que la creación de una cuenta en un sistema, finalice con la notificación de una contraseña o clave de acceso. El apartado dedicado al control de gestión de la información de autenticación secreta de los usuarios[13] proporciona pautas para su correcta y segura notificación.

2.2.5 Tecnologías aplicables

Los procesos formales de alta y baja de un usuario en un sistema se pueden apoyar en cualquier herramienta siempre que cumpla con los siguientes requisitos:

- Permitir un registro y almacenamiento de todas las solicitudes que se realizan.
- Permitir un control de estado de la solicitud.

[12] Ver apartado "*4.4 Utilización de programas o utilidades privilegiadas*" de este documento.

[13] Ver apartado "*2.4 Gestión de la información de autenticación secreta de los usuarios*" de este documento.

- Y que permita la creación de flujos de aprobación automatizados.

Cualquiera de las aplicaciones mencionadas en el apartado anterior, siguen siendo válidas para este control en la medida en que se trata de garantizar la existencia de un proceso de solicitud, validación y autorización. Por tanto, como referencia se puede mantener:

- Remedy[14] o Request Tracker, RT[15], como herramientas de ticketing.
- IBM Security Identity Manager[16] o NetIQ Identity Manager[17], como herramientas expertas en la Gestión de Identidades.

2.2.6 Métricas para el cuadro de mando

Algunas preguntas interesantes para verificar el grado de cumplimiento de este control serían:

- ✓ ¿Existe un proceso formal para solicitar el acceso y la cancelación de acceso a las aplicaciones y sistemas de una organización?
- ✓ ¿Existe una aplicación o herramienta en la que se gestionen automáticamente este tipo de peticiones?
- ✓ ¿Cuántas aplicaciones y sistemas se apoyan en la herramienta de gestión automatizada? ¿Qué porcentaje supone respecto del total existente en la organización?
- ✓ ¿Cuántas aplicaciones y sistemas no utilizan la herramienta de gestión automatizada? ¿Qué porcentaje supone respecto del total existente en la organización?
- ✓ ¿En cuántas aplicaciones y sistemas no disponen ni siquiera de un proceso formal y por tanto quedan fuera del control de la organización?
- ✓ ¿De cuántos identificadores de usuario diferentes requiere un empleado de una organización?

Cuando existe herramienta automática para la gestión de peticiones de acceso, además es interesante identificar la siguiente información, por ejemplo para evaluar mensualmente:

- ✓ Peticiones de acceso:

[14] http://www.bmcsoftware.es/it-solutions/remedy-itsm.html

[15] https://www.bestpractical.com/rt/

[16] http://www-03.ibm.com/software/products/es/identity-manager

[17] https://www.netiq.com/es-es/products/identity-manager/advanced/

- ¿Cuántas peticiones de acceso se reciben?
- ¿Cuál es el tiempo medio de resolución de una petición de acceso?
- ¿Cuántas peticiones están en espera de ser validadas en un instante determinado y cuánto tiempo llevan esperando?
- ¿Cuántas peticiones han sido rechazadas y por qué motivos?
- ¿Cuántas de las peticiones se deben a cambios en el perfil, rol o puesto que desempeña un usuario?

✓ Peticiones de cancelación de acceso:

- ¿Cuántas peticiones cancelación de acceso se reciben?
- ¿Cuál es el tiempo medio de resolución de una petición cancelación de acceso?
- ¿Cuántas se deben a baja en la organización?

Cuando no existe una herramienta para la gestión de peticiones de acceso, pero sí al menos un proceso formal por otras vías, es interesante identificar la siguiente información:

- ✓ ¿Cuántos usuarios existen en la aplicación o sistema?
- ✓ ¿Cuántos usuarios, de entre los existentes, se solicitaron siguiendo las vías formales?
- ✓ ¿Cuántas peticiones han sido rechazadas y por qué motivos? (por ejemplo en el último mes)
- ✓ ¿Cuántas peticiones de baja se han recibido? (por ejemplo en el último mes)
- ✓ ¿Cuántas se deben a baja en la organización?

La existencia de procesos formales para el aprovisionamiento de acceso de usuarios, su penetración entre las aplicaciones y servicios de una organización y la media de identificadores de usuario diferentes que un mismo empleado utiliza dentro de una organización, proporciona un indicador sobre el nivel de madurez de la organización.

La relación entre cuántos usuarios fueron solicitados utilizando el proceso formal y cuántos usuarios existen realmente en los sistemas y aplicaciones, proporciona un indicador sobre la efectividad o grado de uso del proceso de aprovisionamiento. Todo lo que no fueran casos aislados, debería ser tomado por la organización como un riesgo importante contra la seguridad de su organización.

Por otro lado, las métricas respecto a los tiempos medios para resolver una petición. Aunque los tiempos de resolución de petición de acceso pueden ser un indicativo de eficiencia, desde el punto de vista de la seguridad lo que será importante será el tiempo medio para resolver una petición de cancelación de acceso. Tardar mucho en resolverlo significa que existe un usuario activo en algún sitio que no debería ya estarlo, por lo que se trata de un riesgo de seguridad para una organización.

Y por último, las métricas que evalúan el volumen de peticiones de cancelación de acceso. Cuando sus resultados se cruzan con las bajas cursadas por Recursos Humanos de una organización, ofrecería indicadores muy interesantes en cuanto al volumen de cuentas de usuario obsoletas que puede tener una organización. Las cuentas de usuario obsoletas pueden convertirse en un punto débil muy importante para una organización.

2.3 Gestión de los derechos de acceso privilegiados

2.3.1 Definición ISO

La asignación y el uso de derechos de acceso privilegiados deben estar restringidos y controlados.

2.3.2 Guía de implementación ISO

La asignación de derechos de acceso privilegiados debe estar controlada por un proceso formal de autorización que esté alineado con las políticas de control de acceso[18].

Se deben considerar los siguientes pasos:

- Los derechos de acceso privilegiados asociados con cada sistema o proceso (sistema operativo, sistema de administración de bases de datos y cada aplicación) así como a los usuarios a los que se les necesita asignar deben estar identificados.
- Los derechos de acceso privilegiados deben ser asignados a los usuarios en base al criterio de necesidad-de-uso y en base a evento-a-evento, siempre en línea con la política de control de acceso.
- Se debe establecer un proceso de autorización y mantener un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que el proceso de autorización no haya sido completado.
- Se deben definir requisitos para la expiración de derechos de acceso privilegiados.
- Los derechos de acceso privilegiados se deben asignar a un identificador de usuario diferente de aquellos utilizados en actividades de negocio habituales. No se deben realizar actividades de negocio utilizando identificadores de usuarios privilegiados.
- Se deben revisar regularmente las competencias de los usuarios con derechos de acceso privilegiados, con el objetivo de verificar que son acordes a sus tareas.

[18] Ver apartado "*1.1Política de control de accesos*" de este documento.

- Se deben establecer y mantener procedimientos específicos para evitar el uso no autorizado de identificadores de usuarios genéricos de administración en función de las capacidades de configuración de los sistemas.
- Para los identificadores de usuarios genéricos de administración, se debe proteger la confidencialidad de su información de autenticación secreta cuando éstos son compartidos.

2.3.3 Riesgos de seguridad

Disponer de usuarios privilegiados sobre una aplicación o sistema permite no solo acceder, modificar o borrar información, sino además cambiar el comportamiento o los procesos sobre ésta y más importante, permite ocultar las acciones realizadas, ya que se tiene privilegios para desactivar medidas de seguridad, medidas de auditoría y medidas de rastreo.

Por tanto, supone un riesgo directo de la confidencialidad, la integridad y la disponibilidad y permitiendo además la posibilidad de eliminar toda traza de la actividad realizada.

2.3.4 Recomendaciones y Buenas prácticas

El uso inapropiado de usuarios privilegiados es probablemente el riesgo con mayor impacto (atendiendo a criterios técnicos únicamente) que se puede tener, en la medida en que es un usuario que puede hacer (y deshacer) cualquier sistema o configuración y además tiene la posibilidad de no dejar rastro de lo que ha hecho. Por lo que las medidas que requiere la norma son indispensables.

El tratamiento de los usuarios privilegiados que se suele dar según si el sistema se encuentra en un entorno de Desarrollo, un entorno de Preproducción o un entorno Productivo, es completamente diferente. Según se acerque al entorno de Producción, mayor rigurosidad debe aplicarse a dichos usuarios.

El siguiente ejemplo, pretende ilustrar la aplicación de controles exhaustivos para el uso de usuarios privilegiados:

> Una base de datos, sobre la que se apoya una aplicación web que ofrece servicio a los clientes de un banco. Su propia casuística hace evidente la responsabilidad existente en garantizar el correcto funcionamiento e integridad de la base de datos.
>
> En un entorno de Producción, los usuarios administradores de la base de datos, conocidos con DBAs, están desactivados o tienen una contraseña que, quienes actúan como DBAs desconocen. Cuando requieren hacer uso del usuario, por motivo de una incidencia, una actualización de los sistemas o cualquier otra situación que lo requiera, deben hacer una solicitud formal ordinaria para casos

planificados o de emergencia para casos no planificados. Sea cual sea la situación, se exige una solicitud, la cual será enviada a un responsable para su valoración y autorización:

  - Si se autoriza, se asignará una contraseña temporal al usuario DBA, y será notificada al solicitante informándole del período de tiempo que estará activo. Transcurrido el período de tiempo, la contraseña del usuario DBA será cambiada inmediatamente, dejando de ser conocida por tanto por el solicitante y de esa manera, cerrado su acceso.
  - Si no se autoriza, no se haría nada sobre el usuario DBA, puesto que a efectos prácticos el solicitante no la conoce y no puede hacer uso de él.

Siguiendo este tipo de prácticas se garantiza:

- Que el usuario privilegiado es utilizado por una persona, que es identificada e identificable.
- Que el uso del usuario privilegiado es previamente autorizado. No puede ser utilizado libremente.
- Que el uso del usuario privilegiado está acotado y restringido a ventanas de tiempo en general pequeñas, adecuadas únicamente para la labor puntual que se va a realizar con él.
- Cuando no es utilizado el usuario privilegiado, éste se encuentra custodiado adecuadamente.

2.3.5 Tecnologías aplicables

Existen en la actualidad aplicaciones expertas en la custodia y protección de los super-usuarios. Se trata de aplicaciones que guardan y custodian los usuarios privilegiados de sistemas y aplicaciones. Cuando alguien requiere el uso de un usuario privilegiado, debe primero autenticarse ante este sistema experto, el cual decidirá según ciertos criterios o reglas si puede “entregarle” el usuario privilegiado que custodia. Entre los criterios podría estar el solicitar a un responsable autorización antes de entregar un usuario privilegiado.

En general, este tipo de sistemas expertos:

- Garantiza la elección de contraseñas seguras para los usuarios privilegiados, en la medida en que las genera con las máximas características de seguridad que el sistema le permite, por ejemplo, generaría contraseñas de 16 caracteres, utilizando números, letras mayúsculas y minúsculas y además símbolos.
- Restringe el tiempo de uso que se puede hacer con el usuario privilegiado. Cuando finaliza el tiempo previsto de uso del usuario privilegiado, gestionaría el cierre de sesión del usuario además del reemplazo inmediato a una nueva contraseña (y por tanto desconocida para el usuario que instantes antes lo hubiera estado utilizando).

- Proporcionan la capacidad de grabar/registrar la sesión y por tanto de grabar/registrar todas las acciones y movimientos que el usuario haya realizado.

Un ejemplo de este tipo de aplicaciones de control de usuarios privilegiados es IBM Security Privileged Identity Manager[19].

2.3.6 Métricas para el cuadro de mando

Las métricas relacionadas con este control, se tienen que mirar focalizando en el comportamiento de aplicaciones concretas, es decir, extraer métricas únicamente de aquellos sistemas o aplicaciones que puedan ser más críticas para la organización, puesto que extraerlo para todas posiblemente sería una labor inviable para muchas organización. Algunas preguntas interesantes para verificar el grado de cumplimiento de este control serían:

- ✓ ¿Cuántos usuarios privilegiados "personales" existen en el sistema? ¿Qué porcentaje representa respecto del total de usuarios privilegiados "genéricos" del sistema (es decir, usuarios privilegiados que no están directamente asociados a una persona, propietaria del usuario)?
- ✓ ¿Cuántos accesos se realizan con el usuario o usuarios privilegiados (accesos diarios y también acumulados mensuales para cálculo de media de uso)?
- ✓ ¿Qué tipo de acciones se realizan (cuando sea posible identificarlo)?
- ✓ ¿Cuántos intentos de acceso fallidos de usuarios privilegiados se han producido?

Este tipo de métricas proporcionarán una idea a la organización sobre el uso que se hace de sus usuarios privilegiados para determinar si es adecuado o si se utiliza "demasiado", es decir, que se pueda estar utilizando para tareas que no corresponden a este tipo de usuarios.

También el volumen de usuarios privilegiados genéricos utilizados también será un indicador relevante sobre el riesgo que está corriendo una organización, en la medida en que se realizan actividades privilegiadas sin poder precisar quién en particular las ha realizado.

Si se utilizan herramientas de control de usuarios privilegiados, será la propia aplicación quién genere informes sobre los usuarios privilegiados activados, a quién y por cuánto tiempo.

[19] http://www-03.ibm.com/software/products/es/pim

2.4 Gestión de la información de autenticación secreta de los usuarios

2.4.1 Definición ISO

La asignación de la información de autenticación secreta debe estar controlada a través de un proceso de gestión formal.

2.4.2 Guía de implementación ISO

El proceso debe incluir los siguientes requisitos:

- Se debe requerir a los usuarios que firmen una cláusula de que mantendrán sus correspondientes informaciones de autenticación secretas personales confidencialmente y de que cuando se trate de información de autenticación secreta compartida, únicamente lo compartirán con los miembros del grupo. Esta cláusula puede formar parte de los términos y condiciones estipulados en el contrato de los empleados.
- Cuando se requiera que los usuarios mantengan su propia información de autenticación secreta, se les deberá proveer inicialmente con información de autenticación secreta temporal segura, que tengan forzosamente que cambiar tras su primer uso.
- Se deben establecer procedimientos para verificar la identificad de un usuarios antes de entregarle información de autenticación secreta nueva, de reemplazo o temporal.
- La información de autenticación secreta temporal debe entregarse al usuario de una manera segura; la utilización de correos electrónicos inseguros o de terceras personas debe ser evitado.
- La información de autenticación secreta temporal debe ser única para cada usuario y no debe ser predecible.
- Los usuarios deben confirmar acuse de recibo de la información de autenticación secreta que se le entregue.
- La información de autenticación secreta por defecto de productos y sistemas debe modificarse tras su instalación.

2.4.3 Riesgos de seguridad

Una mala gestión de las contraseñas debilita cualquier esfuerzo realizado en el sistema de control de accesos implementado, ya que son el mecanismo más habitual para verificar la identidad de un usuario antes de permitirle su acceso, es decir, para autenticar al usuario y autorizar su acceso.

Por tanto, supone un riesgo directo contra la confidencialidad, integridad y disponibilidad de la información y también contra la trazabilidad en la medida en que aunque se pueda ser capaz de identificar el usuario con el que se realizó una determinada acción, no resulta verdadera la identidad del mismo.

2.4.4 Recomendaciones y Buenas prácticas

Aunque existen muchos mecanismos de autenticación, las contraseñas son el mecanismo de autenticación más utilizado y por tanto es esencial mantener una seguridad óptima sobre ellas en la que participan las propias organizaciones pero también los usuarios:

- Por parte de las organizaciones, es importante que exijan la aplicación de una buena política de contraseñas, pero también es importante la existencia de procesos de gestión de la contraseña que sean seguros.
- Por parte de los Usuarios, deben **entender** la importancia que tienen las contraseñas, **conocer** las medidas de seguridad que la Organización aplica sobre ellas y **asumir** que son responsables de ellas.

El ciclo de vida de una contraseña es sencillo: generación, entrega a su usuario (cuando corresponda), uso y finalmente desactivación o borrado si así procediera. Proteger las contraseñas implica aplicar medidas de seguridad en cada una de estas fases:

- Fase de Generación de contraseñas

  Desde el punto de vista de la seguridad, lo mejor siempre sería que fuera el propio usuario quien eligiera su contraseña. Pero lo habitual es que alguien asigne una contraseña al usuario, al menos cuando se le está creando una cuenta de usuario en un sistema.

  En estos casos, lo recomendable es que estas contraseñas nazcan marcadas para ser de un solo uso, es decir, que el usuario propietario real de la contraseña, en su primer uso, sea obligado a cambiarla y así tener una que pueda considerarse verdaderamente secreta.

  Pero independientemente de quién elija una contraseña, las contraseñas tienen sus propios riesgos:

  - Los usuarios utilizan contraseñas débiles e incluso predecibles.

Por ello, es recomendable que todas las aplicaciones o sistemas obliguen al usuario a elegir contraseñas con un mínimo de calidad y seguridad. Típica es ya la exigencia de un mínimo de 8 caracteres, existencia de números y letras, y también de símbolos.

Pero además del formato de las contraseñas, imposiciones como la caducidad de contraseñas o la imposibilidad de reutilizar contraseñas anteriormente utilizadas, ayuda a elevar el nivel de protección que las contraseñas ofrecen como mecanismo de autenticación y acceso.

- Los usuarios terminan anotando en cuadernos, notas o ficheros sus contraseñas.

  El hecho de obligar a los usuarios a utilizar contraseñas complejas, complica su uso y terminan estando anotadas en cuadernos, notas o ficheros. En este caso no hay manera técnica sencilla de solucionarlo, pero sí hay trucos útiles que se pueden ofrecer a los usuarios para seleccionar de forma sencilla sus contraseñas. Por ejemplo:

- Utilizar las iniciales de cada palabra del título de las películas favoritas del usuario.
- Sustituir de palabras elegidas por el usuario, las letras L o I por el número 1, la letra O por el número 0.
- Intercalar símbolos o signos de puntuación en medio de palabras elegidas por el usuario.
- Etc.

- Fase de Entrega a su usuario

  El estándar destaca el riesgo existente en la entrega de contraseñas a un usuario. El riesgo existente en que se entregue una contraseña a un usuario equivocado es alto, pero en que se entregue a un usuario malicioso lo es más.

  La entrega de una contraseña debe ser un proceso estudiado detenidamente y dependerá mucho de las circunstancias o el contexto de la aplicación o sistema para el que sea, puesto que todos tienen pros y contras:

  - Se puede notificar la contraseña a un responsable del usuario (ámbito laboral). En general se puede considerar que es una persona confiable, pero puede que sea ineficiente el proceso porque en muchas ocasiones los responsables no están siempre disponibles ni a mano de los usuarios.
  - Se puede notificar la contraseña a una cuenta de correo del usuario o a dispositivos personales. Son opciones muy habituales hoy en día de servicios web, redes sociales, etc.
  - Se puede notificar la contraseña en el mismo momento en que se está solicitando. En este caso, el disponer de un mecanismo de autenticación del

usuario alternativo al de la contraseña que se ha pedido generar, es vital para garantizar la seguridad del proceso. Son habituales en estos casos la existencia de las llamadas Preguntas de Verificación.

Con carácter general, siempre debe tomarse la precaución de nunca notificar de manera conjunta un "identificador de cuenta de usuario" junto con la "contraseña" asignada, y si fuera posible, tampoco de a qué servicio o aplicación proporciona el acceso. Cuanto más limitada sea la información, un robo o acceso no autorizado a la misma proporcionará menos utilidad.

Una última medida interesante a este respecto, es que exista una notificación por otra vía diferente a la utilizada para comunicar una contraseña, que informe al usuario de que sea ha realizado una determinada acción sobre su contraseña. De esa manera, si se ha solicitado por ejemplo, una regeneración de la contraseña de manera maliciosa con motivo de que se le ha olvidado la contraseña al usuario, aunque no se puede evitar que ocurra, lo que sí se podrá es detectar a posteriori y así activar otras medidas cautelares en consecuencia.

- Fase de Uso

  El estándar dedica el objetivo de Responsabilidades de los usuarios[20] precisamente a la responsabilidad en el uso y protección de los mecanismos de autenticación que se le proporcionen, por lo que las medidas y recomendaciones que sean de aplicación, se indicarán en dicho apartado.

- Fase de Desactivación o Borrado

  Siempre que una cuenta de usuario deje de ser necesaria, debe borrarse o al menos desactivarse para no ser un riesgo de seguridad para su aplicación o sistema. En ocasiones un simple cambio de contraseña a una que desconozca el usuario puede ser suficiente cuando la desactivación se prevé temporal.

2.4.5 Tecnologías aplicables

La utilización de aplicaciones de gestión de identidades como las mencionadas en apartados anteriores (IBM Security Identity Manager[21] o NetIQ Identity Manager[22], como) es la mejor herramienta en la protección de la información de autenticación secreta como las contraseñas.

[20] Ver apartado "*3 Responsabilidades de los usuarios*" de este documento.

[21] http://www-03.ibm.com/software/products/es/identity-manager

[22] https://www.netiq.com/es-es/products/identity-manager/advanced/

Este tipo de sistemas expertos proporcionan un interfaz adecuado para permitir elegir al usuario sus propias contraseñas con los mínimos de calidad que cada Organización desee. Permiten también la asignación automática de contraseñas iniciales, generadas aleatoriamente y enviadas y notificadas al usuario por los medios que se quieran configurar, y además, dejan registro de toda solicitud y actuación realizada al respecto.

Pero en caso de no disponer de soluciones completas de gestión de identidades, también existen aplicaciones que pretender facilitar la gestión de contraseñas a las Organizaciones garantizando la seguridad. Se trata de aplicaciones que gestionan el reseteo de contraseñas por parte de los propios usuarios y que una vez reseteadas o cambiadas, la propagan a los sistemas o aplicaciones indicadas. Un ejemplo de este tipo de aplicaciones es NetIQ Self Service Password Reset[23].

2.4.6 Métricas para el cuadro de mando

Aunque la custodia de la contraseña que hacen los usuarios no es posible medirla, se pueden tomar en referencia otras métricas que pueden proporcionar una idea a una organización sobre la efectividad de los procesos de gestión de las contraseñas que tienen. Algunas interesantes, por ejemplo para evaluar mensualmente, serían:

- ✓ ¿Cuántas solicitudes de regeneración de contraseñas por olvido se han recibido?
- ¿Cuántas de esas solicitudes se han detectado que fueran fraudulentas o maliciosas?
- ✓ ¿Cuántas solicitudes de desbloqueo de contraseñas o cuentas se han recibido?
- ¿Cuántas de esas solicitudes se han detectado que fueran fraudulentas o maliciosas?

2.5 Revisión de los derechos de acceso de los usuarios

2.5.1 Definición ISO

Los propietarios de activos deben revisar los derechos de acceso de sus usuarios a intervalos regulares.

2.5.2 Guía de implementación ISO

La revisión de los derechos de acceso debe considerar lo siguiente:

[23] https://www.netiq.com/products/self-service-password-reset/

- Los derechos de acceso de los usuarios se deberían revisar a intervalos de tiempo regulares y cuando se produzca cualquier cambio significativo como promociones de los trabajadores, despidos, etc.
- Los derechos de acceso de los usuarios se deberían revisar y/o reasignar cuando se produzcan cambios de rol de algún trabajador.
- Las autorizaciones de los derechos de acceso privilegiados se deberían revisar a intervalos de tiempo regulares incluso menores que los de los restantes usuarios.
- La asignación de privilegios debería revisarse regularmente para asegurar que no se han obtenido privilegios no autorizados.
- Cambios de cuentas privilegiadas deberían registrarse en logs para su revisión posterior periódica.

2.5.3 Riesgos de seguridad

El principal riesgo de no hacer una revisión de los derechos de acceso de los usuarios es que se mantienen permisos, privilegios e incluso cuentas de usuario que no deberían estar ni tener acceso (habitualmente por obsolescencia del derecho de acceso). Esta situación provoca un riesgo contra la confidencialidad, integridad y disponibilidad de la información.

2.5.4 Recomendaciones y Buenas prácticas

A pesar de que existan procedimientos (u obligaciones) para gestionar un cambio o baja de un derecho de acceso, es muy frecuente que se produzcan las siguientes situaciones:

- Existen cuentas de usuarios que ya no están en la compañía…porque no se les dio de baja convenientemente.
- Un usuario solicitó privilegios mayores de manera temporal… y nunca se retornó a la situación inicial.
- Un usuario posee un acceso indebido… porque se evaluó su solicitud de manera errónea o porque cambio de puesto y requería un ajuste de sus permisos.
- El usuario se auto-asignó privilegios haciendo uso de otro usuario privilegiado.

Como este tipo de situaciones puede darse, aun contando con procedimientos de gestión de usuarios adecuados, la existencia de procesos periódicos de revisión (y limpieza) de usuarios es importante para cualquier organización, pero más representativo cuanto mayor sea ésta por el impacto que la existencia de usuarios indebidos puede causarle.

La forma en que las cuentas de acceso y los privilegios están asignados, puede hacer que los procesos de revisión en busca de usuarios obsoletos o erróneos se conviertan en un

proceso sencillo o un proceso complejo y habitualmente costoso, en cuyo caso una organización por tanto puede decidir que no le compense. Por ejemplo:

- Una organización en que los privilegios otorgados dependen directamente de permisos específicos por aplicación, es decir, de bajo nivel, resultaría tedioso y lento de revisar. Sólo con el conocimiento experto del responsable de la aplicación y de su información es capaz de identificar permisos elevados otorgados a un usuario.
- En cambio, una organización en que los privilegios otorgados están organizados en base a roles o perfiles volcados en repositorios comunes, facilita enormemente el proceso de revisión, permitiendo incluso una automatización directa.

2.5.5 Tecnologías aplicables

No hay tecnologías concretas para resolver este tipo de cuestión en particular. En general, en la medida en que una organización tenga implantados sistemas de gestión de identidades, así será de fácil resolver la aplicación de este control mediante simples scripts de comparación ejecutados periódicamente o que envíen listados de usuarios a los responsables de información para su verificación.

Cuanta menos gestión de identidades organizada se realice, más complicada la ejecución de la tarea.

2.5.6 Métricas para el cuadro de mando

Las métricas más importantes para una Organización en este control es precisamente conocer de la existencia de cuentas obsoletas, cuentas huérfanas o cuentas mal privilegiadas. La evolución de estos datos en el tiempo también será una métrica importante que le indique la efectividad de los procesos de limpieza que deberían ir asociados. Por tanto, de manera periódica sería interesante identificar las siguientes métricas:

- ✓ ¿Se realizan procesos de revisión periódicos?
- ✓ ¿Cuántas cuentas obsoletas se han identificado y qué porcentaje supone respecto del total de cuentas existente?
- ✓ ¿Cuántas cuentas sin propietario se han identificado y qué porcentaje supone respecto del total de cuentas existente?
- ✓ ¿Cuántas cuentas con exceso de privilegios se han identificado y qué porcentaje supone respecto del total de cuentas existente?
- ✓ Crecimiento o decrecimiento de las métricas anteriores respecto a periodos de revisión anteriores.

2.6 Eliminación o ajuste de derechos de acceso

2.6.1 Definición ISO

Los derechos de acceso de todo empleado o de usuarios de terceros externos a la información o a cualquier utilidad de procesado de información deben ser eliminados tan pronto termine el empleo, contrato o acuerdo, o ajustados en función de los cambios.

2.6.2 Guía de implementación ISO

En el caso de terminación es importante eliminar o bloquear los derechos de acceso del usuario. En el caso de cambios, los derechos de acceso deben adecuarse a dichos cambios, lo que implica eliminar unos y asignar otros.

Los derechos de acceso a considerar incluyen tanto los lógicos como los físicos, lo que puede incluir la eliminación, la revocación o la sustitución de claves, tarjetas de identificación, herramientas de procesado de información o suscripciones. Cuando el usuario tuviera conocimiento de identificadores de usuarios compartidos o genéricos y de su correspondiente información de autenticación secreta, ésta deberá ser también cambiada.

Cualquier documentación que identifique los derechos de acceso de los usuarios debe reflejar el cambio o eliminación.

Por último, se destaca que puede haber situaciones en las que convenga reducir, modificar o eliminar derechos de acceso de un usuario antes de que se produzca la terminación de la relación o el cambio, dependiendo de la evaluación de factores de riesgo como:

- En función del motivo de la terminación y en función de si la terminación o el cambio es iniciado por el empleado, el usuario externo o por su gerencia. Pueden provocarse situaciones de intención de sabotajes, robos de información, destrucción de información, etc.
- En función de las responsabilidades actuales del empleado, el usuario externo u otro tipo de usuario.
- En función del valor del activo actualmente accesible.

2.6.3 Riesgos de seguridad

El principal riesgo de no actualizar convenientemente los derechos de acceso de usuarios que abandonan por cualquier motivo una organización, es que se seguiría permitiendo su

posible acceso con el agravante de que podría utilizarse con fines maliciosos o de despecho: sabotajes, robos de información, destrucción de información, pérdidas de servicio, etc.

Esta situación provoca un riesgo contra la confidencialidad, integridad y disponibilidad de la información.

2.6.4 Recomendaciones y Buenas prácticas

La necesidad de inmediatez de ejecutar y propagar la baja de un usuario es obvia. En muchas organizaciones la baja no necesariamente significa un borrado o eliminación del usuario. En muchas ocasiones una baja tiene que programarse como un "bloqueo definitivo" del usuario. El motivo es que si se realiza una eliminación total del usuario, en caso de necesidad de futuras investigaciones, podría perderse información importante que permitiera identificar al usuario. Por tal motivo, una baja es más recomendable que sea implementada como un bloqueo definitivo, pero consultable en caso necesario.

Por otro lado, para garantizar el cumplimiento efectivo de este control que trata de prevenir posibles sabotajes o robos, resulta idónea la utilización de sistemas de gestión de identidades como ya se comentó en el apartado referido al aprovisionamiento de permisos de acceso.

La existencia de este tipo de sistemas controla los usuarios desde el origen hasta el final de las ramificaciones que se crean a través de sistemas. Por tanto, cuando se marca una baja, ésta se propaga automáticamente a lo largo de los sistemas de la organización. La penetración de la orden es mucho mayor (aun cuando pueda haber sistemas o aplicaciones no integradas en la gestión de identidades) frente a que se delegue en los diferentes administradores de las aplicaciones o sistemas, puesto que un responsable no tiene porqué acordarse o conocer todos los sistemas en los que su antiguo empleado podría haber llegado a tener acceso.

2.6.5 Tecnologías aplicables

Cualquiera de las aplicaciones mencionadas en apartados anteriores para la gestión de identidades, como IBM Security Identity Manager[24] o NetIQ Identity Manager[25], como herramientas expertas en la Gestión de Identidades.

[24] http://www-03.ibm.com/software/products/es/identity-manager

[25] https://www.netiq.com/es-es/products/identity-manager/advanced/

2.6.6 Métricas para el cuadro de mando

Cualquier métricas que pueda resultar interesante en este contexto, estaría relacionada con las sugeridas en el control sobre aprovisionamiento de acceso de usuarios[26].

[26] Ver apartado "*2.2 Aprovisionamiento del acceso de usuarios*" de este documento.

3. Responsabilidades de los usuarios

ISO/IEC 27002:2013 establece como objetivo para las responsabilidades de los usuarios el que sean responsables de salvaguardar su información de autenticación.

3.1 Uso de información de autenticación secreta

3.1.1 Definición ISO

Se debe requerir a los usuarios que sigan las prácticas y recomendaciones de la organización en cuanto a uso de la información de autenticación secreta.

3.1.2 Guía de implementación ISO

Todos los usuarios deberían estar asesorados sobre:

- Mantener su información de autenticación secreta de manera confidencial, asegurándose de que no la divulgan con terceras personas.
- Evitar guardar o escribir o mantener un registro de las informaciones de autenticación secretas que puedan tener (ni en papeles, ni en ficheros ni en dispositivos de mano), a menos que puedan ser almacenados de manera segura y el mecanismo de almacenamiento haya sido aprobado por la compañía (por ejemplo con el uso de aplicaciones de custodia de contraseñas, “password vault”).
- Cambiar la información de autenticación secreta ante cualquier indicio de que ha podido ser comprometida.
- Cuando se utilicen contraseñas como mecanismo de información de autenticación secreta, seleccionar contraseñas de calidad, con suficiente longitud mínima y que:
    - Sean fáciles de recordar.
    - No estén basadas en nada que alguien pueda fácilmente averiguar o que se pueda intuir por ser información asociada a la propia persona (por ejemplo, nombres, fechas de nacimiento, números de teléfono, etc.).
    - No sean vulnerables a ataques de diccionario.
    - No sean todo numéricas o todo alfabéticas.
    - Y si son temporales, que se cambien tras el primer uso o inicio de sesión.
- No compartir la información de autenticación secreta.

- Asegurar protección adecuada a las contraseñas cuando éstas son utilizadas como información de autenticación secreta en procesos automáticos con inicio de sesión y que las almacenen.
- No utilizar la misma información de autenticación secreta en el entorno de negocio que en el entorno personal.

La norma también advierte de que el uso de Single Sign On (SSO) o de otras herramientas de gestión de información de autenticación secreta puede reducir la cantidad de información de autenticación secreta que los usuarios tienen que proteger, lo que puede aumentar la efectividad de este control, pero por el contrario, este tipo de herramientas incrementan el impacto en caso de que revele o descubra la información de autenticación secreta de un usuario.

3.1.3 Riesgos de seguridad

El uso de información de autenticación secreta débil o sin la protección ni el cuidado adecuado supone un riesgo contra la confidencialidad de la información, su integridad y su disponibilidad en la medida en que la autenticación se puede considerar anulada.

La trazabilidad en sí no se ve afectada, aunque sí falseada, puesto que la identidad del causante de una determinada acción se puede seguir identificando, pero ésta identificación resultará falsa.

3.1.4 Recomendaciones y Buenas prácticas

Tan importante como haber exigido un mínimo de calidad en la generación y en la distribución de la contraseña, es ahora que el usuario la mantenga en secreto durante todo el tiempo en que la tiene que utilizar y para ello la mejor medida consiste en informar y concienciar al usuario en ello:

- No debe compartir sus contraseñas.
- No debe anotarlas en notas o ficheros, sino que debe ser capaz de recordarlas.

Es recomendable elaborar pequeñas guías que proporcionen a los usuarios un mecanismo sencillo para que inventen sus propias contraseñas pero con unas ciertas garantías. De esa manera, el usuario no sólo elegirá convenientemente sus contraseñas sino que además no supondrán un problema para él por constantes olvidos, por equivocaciones al teclearlas, etc…

Por ejemplo, algunas indicaciones o ideas que se pueden dar para elegir una buena contraseña serían las siguientes:

- Que utilice para la contraseña una palabra rara inventada o el acrónimo de alguna frase hecha que le guste.

- Utilizar sílabas de una canción o un poema que conozca el usuario.
- Que piense en una frase larga que pueda recordar y después que seleccione para la contraseña la primera letra de cada una de las palabras de la frase

Pero a lo largo del tiempo de uso de la contraseña, pueden suceder acontecimientos que hagan u obliguen a que la contraseña se cambie:

- Se le olvida la contraseña al usuario.
- Se le bloquea la contraseña por reintentos de autenticación fallidos consecutivos.
- Se cumplen la caducidad prevista de la contraseña.
- El usuario sospecha de que alguien ha descubierto su contraseña.
- El usuario simplemente quiere cambiarla y utilizar una nueva.

Cualquiera de estas situaciones debe acogerse a las recomendaciones de seguridad que se indicaron para la gestión de contraseña[27].

Existen muchos estudios que destacan la carga de trabajo y por tanto pérdida de rentabilidad que los olvidos y bloqueos de contraseñas pueden llegar a suponer para las Organizaciones y por este motivo, muchas Organizaciones dedican grandes esfuerzos en facilitar la vida a sus usuarios. En función de la Organización, se pueden adoptar unas u otras medidas con este objetivo:

Por ejemplo, si una Organización es joven, incipiente, una forma sencilla de facilitar la gestión de las contraseñas, es hacer converger todas las aplicaciones y sistemas para que utilicen un repositorio de usuarios y por tanto de autenticación común. Es decir, típicamente que se integren con el Directorio Activo de Windows o con un LDAP corporativo. Aunque esta solución no elimina el que el usuario tenga que autenticarse ante cada aplicación o sistema al que quiera acceder, sí le facilita el que siempre utilizará las mismas credenciales de autenticación.

En cambio, si una organización ya tiene mucho recorrido y multitud de aplicaciones o sistemas, probablemente promover el cambio al uso de un repositorio común de autenticación no es una opción. En estos casos, la solución es el uso de herramientas de Single Sign-On. El propio estándar destaca el incremento del impacto en caso de descubrimiento de una contraseña, pero en su favor tienen la optimización de la productividad. Además, los riesgos por descubrimiento de contraseñas cuando se utilizan herramientas de Single Sign-On pueden compensarse con otros controles que permiten minimizar tales impactos, por lo que su aplicación es interesante y ventajosa:

- Forzar a realizar cambios de contraseña con más frecuencia.
- Forzar a elegir contraseñas de más calidad.

[27] Ver apartado "*2.4 Gestión de la información de autenticación secreta de los usuarios*" de este documento.

- Monitorear el uso de las contraseñas en sistemas en busca de patrones de ataques, como accesos fuera de hora, accesos masivos a información, accesos desde diferentes IPs simultáneamente… el uso de herramientas SIEM ayudaría en este aspecto, por ejemplo.

3.1.5 Tecnologías aplicables

Desde el punto de vista del usuario, y precisamente porque en la actualidad el usuario dispone cada vez de más aplicaciones y servicios a los que accede siendo tanto de su ámbito laboral como de su ámbito personal, existen aplicaciones que pretenden convertirse en una "cartera de contraseñas", protegiendo el almacenamiento de éstas con algoritmos criptográficos. Algunos ejemplos de este tipo de aplicaciones son LockCrypt[28] o 1Password[29], y en algunos casos, pueden incluso ser recomendadas por las propias Organizaciones cuando no hacen uso de sistemas de Single Sign-On.

Y desde el punto de vista de las Organizaciones, soluciones de Single Sign-On hay muchas. Prácticamente cualquier fabricante reconocido dispone de una:

- IBM Security Access Manager for Enterprise Single Sign-On[30]
- NetIQ SecureLogin[31]
- NetIQ Access Manager for Web applications[32]

3.1.6 Métricas para el cuadro de mando

Aunque la custodia de la contraseña que hacen los usuarios no es posible medirla, se pueden tomar en referencia otras métricas que pueden proporcionar una idea a una organización sobre cómo gestionan y utilizan sus usuarios sus contraseñas. Algunas interesantes, por ejemplo para evaluar mensualmente, serían:

- ✓ ¿Cuántos intentos de autenticación fallidos se han producido? (para ciertas aplicaciones o sistemas que la organización considere críticos o importantes para analizar).

[28] http://www.lockcrypt.com/

[29] https://agilebits.com/onepassword

[30] http://www-03.ibm.com/software/products/en/access-mgr-esso

[31] https://www.netiq.com/products/securelogin/

[32] https://www.netiq.com/products/access-manager/

- ✓ ¿Cuántos bloqueos de cuenta por exceder el número de intentos de autenticación fallidos consecutivos permitidos se han producido? (para ciertas aplicaciones o sistemas que la organización considere críticos o importantes para analizar).
- ✓ ¿Cuántas solicitudes de regeneración de contraseñas por olvido se han recibido?
- ¿Cuántas de esas solicitudes se han detectado que fueran fraudulentas o maliciosas?
- ✓ ¿Cuántas solicitudes de desbloqueo de contraseñas o cuentas se han recibido?
- ¿Cuántas de esas solicitudes se han detectado que fueran fraudulentas o maliciosas?

4. Control de acceso a sistemas y aplicaciones

ISO/IEC 27002:2013 establece como objetivo del control de acceso a sistemas y aplicaciones el prevenir el acceso no autorizado a éstos.

4.1 Restricción de acceso a la información

4.1.1 Definición ISO

Se debe restringir el acceso a la información y a las funciones del sistema de aplicación en concordancia con la política de control de acceso[33].

4.1.2 Guía de implementación ISO

Las restricciones de acceso deben basarse en requisitos individuales de la aplicación de negocio y en concordancia con la política de control de acceso definida.

Se debe considerar lo siguiente cuando se definan los requisitos de restricción de acceso:

- Establecer menús para controlar los accesos a las funciones del sistema de la aplicación.
- Controlar qué datos pueden ser accedidos por cada usuario particular.
- Controlar los derechos de acceso de los usuarios (por ejemplo, lectura, escritura, borrado y ejecución).
- Controlar los derechos de acceso de otras aplicaciones.
- Limitar la información contenida en las salidas de las aplicaciones o sistemas.
- Proveer controles de acceso lógicos y también físicos para aislar sistemas, aplicaciones o datos de aplicaciones que sean sensibles.

[33] Ver apartado "*1.1Política de control de accesos*" de este documento.

4.1.3 Riesgos de seguridad

No restringir el acceso a la información es un riesgo contra la confidencialidad de la misma en primer lugar y después contra su integridad y/o disponibilidad, independientemente de cómo se acceda a ella.

4.1.4 Recomendaciones y Buenas prácticas

Las aplicaciones y sistemas deben aplicar restricciones de acceso a la información, a las funciones, los menús de aplicaciones e incluyo pantallas de la aplicación en base a la comprobación de derechos de acceso suficientes.

Esta comprobación deben hacerla independientemente de que quién acceda sea un usuario, un usuario privilegiado, un proceso automático originado desde otra aplicación o alguna herramienta, prestación o software con el que se compartan recursos y/o alojamiento físico. Se debe controlar todo tipo de acceso y se debe aplicar un control de Autorización.

En grandes organizaciones, igual que hay gran presencia de sistemas de gestión de identidades, existe gran presencia de sistemas expertos en control de accesos. Se trata de sistemas que se ponen por delante de las aplicaciones de una organización y que se convierten en el punto de acceso a las aplicaciones. El sistema experto se encarga de autenticar al usuario primero y después de verificar si el usuario tiene autorización para acceder al sistema o aplicación solicitado por el usuario. Si dicha verificación es correcta, entonces se encarga de transmitir a la aplicación o sistema final la identidad del usuario y el perfil de autorización que en la aplicación tiene.

Ahora ya es responsabilidad de la aplicación o sistema final el mostrar al usuario la información, menús o pantallas que por su perfil o privilegio le corresponde.

El uso de sistemas expertos de control de acceso no elimina la necesidad (y responsabilidad) que las aplicaciones y sistemas finales tienen con respecto a verificar la existencia de un determinado nivel de autorización y mostrar o dejar actuar en consecuencia de dicho nivel de autorización.

El estándar recoge también la necesidad de aplicación de controles lógicos y físicos de aislamiento:

- Desde el punto de vista del aislamiento físico, hoy en día, casi cualquier organización al menos mediana, utiliza ya salas especializadas para el alojamiento adecuado de sus sistemas o a grandes escalas, Centros de Proceso de Datos, CPDs. El uso de salas especializadas y CPDs proporciona un aislamiento físico de los servidores y por tanto del acceso a los sistemas para posible vulneración de éstos. El estándar cuenta con un dominio específico para este tema denominado

"*Seguridad física y Ambiental*" en el que se profundiza en este tipo de cuestiones y que por tanto queda fuera del alcance de este documento.

- Desde el punto de vista del aislamiento lógico, el estándar también cuenta con un dominio específico para este tema denominado "*Seguridad de las comunicaciones*". En este dominio se propone como control la segregación de redes en base a algún criterio que la Organización desee. El estándar ejemplifica sugiriendo la segregación en base a áreas de negocio, en base a unidades organizativas de la empresa, etc.
- Pero, muchas empresas a día de hoy utilizan otros criterios para su segmentación de las redes. Ese criterio se basa en separar el mundo de las aplicaciones del mundo de los usuarios, y considerar para el mundo de las aplicaciones las recomendaciones y buenas prácticas existentes para el desarrollo de aplicaciones que comienzan con segmentar en tres capas las aplicaciones (Arquitectura de tres capas) para luego separarlo en redes y servidores de capas similares:

  a) Capa de presentación.

  b) Capa de negocio.

  c) Capa de datos.

  Con esta separación en capas y redes, el acceso indebido a una de las capas, no vulnera directamente el acceso a las demás.

  Por tanto, con las arquitecturas de tres capas tan presentes en la actualidad, una segmentación de redes habitual proporciona las siguientes ventajas o medidas de seguridad:

  - Separa la información pública de la interna mediante la creación de una zona desmilitarizada externa, conocida como DMZ. Muchas organizaciones necesitan ofrecer por internet acceso a servicios o información tanto a clientes como a empleados. En la DMZ se ubican las capas de presentación de las aplicaciones que vayan a ser accesibles por internet.
  - Y una vez dentro de la Organización, se siguen diferenciando y separando redes. Algunas habituales son:
    - Una red de backend, en la que se ubica la capa de negocio de las aplicaciones, así como cualquier herramienta o software requerido por la Organización.
    - Una red de datos, en la que se ubica la capa de datos con sus correspondientes bases de datos y repositorios de información y de usuarios.
    - Una red de gestión, dedicada para que los administradores puedan acceder a las páginas y utilidades de administración de aplicaciones y sistemas desde una red segura, asilada de los usuarios con sus propias medidas de seguridad.

- Una red de usuarios o de red interna, en la que se ubican los PCs y portátiles de los empleados.

4.1.5 Tecnologías aplicables

Las soluciones expertas en control de accesos, en general están separadas por la tecnología o más bien por el contexto que son capaces de proteger. Se diferencian entre control de acceso a aplicaciones web y control de acceso a aplicaciones de escritorio.

Los sistemas de control de acceso a aplicaciones web se caracterizan por presentar un portal de autenticación de usuario web, común para todas las aplicaciones que protegen. No se podrá acceder sin que el usuario haya pasado y obtenido la consiguiente autorización de acceso en dicho portal.

Algunos ejemplos de este tipo de tecnologías son:

- IBM Security Access Manager for Web[34]
- NetIQ Access Manager for Web applications[35]

Los sistema de control de acceso a aplicaciones de escritorio en cambio no pueden hacer uso de un interfaz tan estandarizado con son las aplicaciones web y su protocolo de comunicaciones http. En este tipo de sistemas, la variedad de tecnologías y de mecanismos de autenticación propios, hace que tengan su propia complejidad específica. Este tipo de sistemas también tienen un portal de autenticación propio, que servirá de único sistema de autenticación de usuarios y de su correspondiente verificación. Pero en esta ocasión, al no utilizar un entorno estándar web y comunicaciones estándar http o https, para “propagar” la identificación de los usuarios hasta las aplicaciones, estos sistemas se basan en “recordar” el diseño utilizado por la aplicación de escritorio, es decir, ubican físicamente en la pantalla el campo que correspondería a introducir un identificador de usuario y el campo que correspondería a introducir una contraseña. El sistema experto inyecta dichas credenciales en nombre del usuario, y delega la verificación de autorización de bajo nivel a la aplicación.

Algunos ejemplos de este tipo de tecnologías son:

- IBM Security Access Manager for Enterprise Single Sign-On[36]
- NetIQ SecureLogin[37]

[34] http://www-03.ibm.com/software/products/en/access-mgr-web/

[35] https://www.netiq.com/products/access-manager/

[36] http://www-03.ibm.com/software/products/en/access-mgr-esso

[37] https://www.netiq.com/products/securelogin/

4.1.6 Métricas para el cuadro de mando

En otros apartados, ya se proporcionaron métricas referentes a los procesos de autenticación correctos y fallidos. Al ser la autorización el subsecuente paso, las métricas que se deben obtener tienen que estar relacionadas con el objetivo de identificar cuántos intentos de acceso a aplicaciones, funcionalidades, menús, opciones o información de una aplicación se ha tratado de realizar acceso sin tener permiso para ello. Es decir, dando por hecho que el proceso de autenticación fue correcto, pero no la autorización:

- ✓ ¿Cuántas denegaciones de acceso se han producido por no disponer de autorización en la aplicación o sistema?
- ✓ ¿Cuántos intentos de acceso a información, funcionalidades, menús o pantallas correspondientes a perfiles o privilegios mayores que los que tuviera el usuario se han realizado?

Una situación en la que este control y su métrica resultan de vital importancia en cuando se implantan controles de seguridad para el cumplimiento con la LOPD, en particular cuando se tratar datos de los más críticos, lo de nivel alto. Por ley, el acceso a este tipo de datos siempre tiene que quedar registrado y ser auditado. Por lo que intentos de acceso a este tipo de información de manera fraudulenta pueden ser un serio problema para una organización.

4.2 Procedimientos de log-on seguro

4.2.1 Definición ISO

El acceso a aplicaciones y servicios debería estar controlado por un proceso de conexión seguro, cuando así sea requerido por la política de control accesos[38].

4.2.2 Guía de implementación ISO

Se debe elegir una técnica de autenticación adecuada para corroborar la identidad declarada por los usuarios.

Cuando se requiera autenticación y verificación de la identidad robusta se deben utilizar mecanismos alternativos a las contraseñas, con medios criptográficos, como smartcards, tokens o de reconocimiento biométrico.

[38] Ver apartado "*1.1Política de control de accesos*" de este documento.

El procedimiento para iniciar sesión en un sistema o aplicación debe ser diseñado para minimizar la posibilidad de tener accesos no autorizados. El procedimiento de inicio de sesión debe minimizar la información que muestra del sistema o aplicación, de cara a evitar proporcionar a los usuarios no autorizados asistencia innecesaria.

Un buen procedimiento de inicio de sesión debe:

- No mostrar identificación de la aplicación o del sistema hasta que el proceso de inicio de sesión no haya finalizado correctamente.
- Mostrar mensaje o aviso de que el sistema u ordenador sólo puede ser accedido por usuarios autorizados.
- No ofrecer mensajes de ayuda durante proceso de conexión que puedan ayudar o dar pistas a un usuario no autorizado.
- Validar la información de autenticación sólo cuando se hayan introducido todos los datos necesarios. Si se produce un error de autenticación, el sistema no debe indicar qué parte de los datos es el erróneo.
- Proteger contra intentos de autenticación por fuerza bruta.
- Dejar registro de los intentos de inicios de sesión correctos y también fallidos.
- Lanzar o enviar un aviso o alerta de seguridad cuando se detecte una potencial brecha en el control del inicio de sesión.
- Mostrar la siguiente información tras completar conexión con éxito:
    - Fecha y hora de la anterior conexión con éxito
    - Detalles sobre cuando intento de inicio de sesión fallido desde la última conexión correcta realizada.
- No mostrar por pantalla la contraseña que se escribe.
- No transmitir en claro ninguna contraseña por red.
- Finalizar las sesiones que estén inactivas tras un periodo definido de inactividad, especialmente en ubicaciones de alto riesgo como pueden ser áreas públicas o externas a la organización o en dispositivos móviles.
- Restringir los tiempos de conexión para proporcionar seguridad adicional en aplicaciones de alto riesgo y reducir las ventanas de oportunidad para accesos no autorizados.

4.2.3 Riesgos de seguridad

No utilizar procedimientos de log-on seguros debilita todo intento de control del proceso de autenticación y su consecuente acceso, por lo que debilita la confidencialidad, integridad e incluso disponibilidad de la información o servicio accedido.

4.2.4 Recomendaciones y Buenas prácticas

Por el hecho de ser un elemento accesible y punto de entra a un sistema, aplicación o información, el proceso de autenticación es el componente más vulnerable para la seguridad de un sistema, aplicación o información.

La robustez que un proceso de autenticación necesita obviamente depende de la criticidad de los datos gestionados. Las recomendaciones que propone el estándar son muy indicadas para cualquier proceso de autenticación y con frecuencia aplicadas en las organizaciones puesto que previenen de ataques de fuerza bruta entre otras vulnerabilidades que el proceso puede tener.

Los mecanismos de autenticación considerados robustos en comparación con el uso de contraseñas como los certificados o los tokens, proporcionan un mayor nivel de seguridad, pero en contextos de servicios o aplicaciones orientados a clientes, el uso de contraseñas sigue siendo el principal mecanismo utilizado.

En esta situación, en función de la naturaleza de la aplicación y del contexto alrededor de su tipo de usuario, a veces se pueden producir situaciones de ataque extraordinarias que deben contemplarse de manera especial y que las medidas sugeridas por el estándar no previenen ni necesariamente alertan convenientemente. Por ejemplo, las aplicaciones de banca online. Actualmente han evolucionado mucho y los niveles de protección y seguridad aplicados son muy altos. Se debe a la detección y tratamiento de situaciones extraordinarias de ataques a las que se tuvieron que enfrentar en el pasado y que a día de hoy son un buen ejemplo para remarcar que se debe analizar el contexto de uso personal y no sólo técnico que se hace de ciertas aplicaciones y sistemas.

Es frecuente que el acceso a una cuenta bancaria sea realizado por el propietario de una cuenta o por alguno de sus autorizados (habitualmente la pareja o conyugue del propietario). Pero, ¿qué sucede en los casos en que hay separaciones? Pues en ocasiones ocurría que se producían intentos de acceso a cuentas bancarias por parte de las exparejas. Los ataques de fuerza bruta de estas situaciones para tratar de acceder a una cuenta a la que ahora ya no tenían acceso, se caracterizaba porque en los logs se veía el campo correspondiente al número de cuenta siempre fijo y la variable cambiante era únicamente la contraseña. Coincidía además, que los “ataques” provenían siempre desde la misma IP, por no tratarse de un ataque profesional.

Cuando los ataques a las aplicaciones bancarias eran profesionales, solían tener otra caracterización. Trataban de explotar el hecho de que los usuarios utilizaban contraseñas débiles y predecibles, por lo que los ataques solían consistir en que la contraseña se fijaba (por ejemplo a “password”, o a “123456”) y lo que variaba era el número de cuenta bancaria.

Detectar estos ataques diferentes, permitió en su momento aplicar medidas específicas y evolucionar los procesos de autenticación hasta el punto en que se encuentran hoy en día, en base a un PIN largo, con posiciones diferentes en cada acceso e incluso con

teclado en la propia página para eliminar posibles detecciones de contraseñas por lectura del teclado físico.

4.2.5 Tecnologías aplicables

Existen muchas tecnologías que proporcionan mecanismos de logon más seguros que los procesos de autenticación habituales basados en contraseñas. Algunos de ellos son:

- Autenticación con certificados en tarjetas inteligentes (smartcards).
  - Gemalto eToken PRO SmartCard[39]
  - FNMT-CERES. Tarjeta criptográfica FNMT-RCM[40]
- Autenticación con token. Reemplaza la autenticación con usuario y contraseña por la necesidad de autenticarse mediante la inserción de un hardware (una llave USB especial, una smartcard, una etiqueta RFID, etc):
  - Rohos logon key[41]
- Autenticación con one time password. Sistemas que generan una contraseña única válida por períodos de tiempo muy breves, conocidas como contraseñas de un solo uso.
  - McAfee One Time Password[42]
  - Gemalto eToken PASS[43]
- Autenticación biométrica. Consiste en autenticarse ante un sistema por lo que uno es. Mediante técnicas matemáticas y estadísticas se es capaz de identificar a una persona por un rasgo físico, como su huella dactilar, el iris de su ojo, su rostro, su voz o la geometría de la mano, por ejemplo.
  - Kimaldi Suprema Face Station, para reconocimiento facial[44]
  - ElevenPaths, SmartID para huella dactilar[45]

---

39 http://www.safenet-inc.com/multi-factor-authentication/authenticators/pki-smart-cards/etoken-pro-smart-card-security/

40 https://www.cert.fnmt.es/catalogo-de-servicios/tarjetas-criptograficas

41 http://www.rohos-es.com/productos/rohos-logon-key/

42 http://www.mcafee.com/es/products/one-time-password.aspx

43 http://www.safenet-inc.com/multi-factor-authentication/authenticators/one-time-password-otp/etoken-pass/

44 http://www.kimaldi.com/productos/sistemas_biometricos/huella_vascular_y_facial/biometria_facial

45 https://www.elevenpaths.com/es/tecnologia/smartid/index.html

- Nuance Voice Biometrics[46]

4.2.6 Métricas para el cuadro de mando

Evaluar el cumplimiento de las recomendaciones proporcionadas por el estándar para obtener un proceso de logon seguro es más un proceso de revisión y auditoría de que se cumplen los requerimientos técnicos en los procesos de las diferentes aplicaciones.

A una organización en realidad la métrica que le interesará será conocer el resultado de esa auditoría evaluando que lo cumplen. Por tanto, las métricas para este control serían:

- ✓ ¿En cuántos sistemas de la organización el proceso de logon cumple las directrices del estándar? ¿qué porcentaje supone respecto al total?
- ✓ ¿En cuántos sistemas de la organización el proceso de logon no cumple las directrices del estándar? ¿qué porcentaje supone respecto al total?
- ✓ ¿Cuántos sistemas de la organización están pendientes de evaluar?

Ahora bien, en función del mecanismo de autenticación utilizado por las aplicaciones, puede ser interesante evaluar su grado de precisión y por tanto de seguridad que ofrece a la organización. Es decir:

- Si se utiliza como mecanismo de autenticación el basado en “Usuario y Contraseña”, la efectividad del control ya se repasó en anteriores apartados.
- Si se utilizan sistemas de autenticación biométricos, quizás las métricas más importantes serían:
- ¿Cuántas llamadas al servicio de atención al usuario/empleado se han recibido indicando que no han podido autenticarse con el sistema biométrico? Este volumen proporcionará un indicador sobre cuántos falsos negativos se han producido y por tanto el impacto que está teniendo el sistema de autenticación por falta de precisión.
- ¿Cuántos accesos indebidos es capaz de identificar un responsable de una aplicación tras revisar un log de accesos? Este dato, bastante complejo de identificar con precisión, sería el que proporcionaría un indicador sobre posibles accesos fraudulentos que se han sufrido. La organización no puede hacer nada por evitar ese acceso concreto, puesto que ya ocurrió, pero un volumen alto sería un indicador de que el sistema de autenticación está fallando.
- Si se utilizan certificados, métricas interesantes para la organización sería identificar:

[46] http://www.nuance.es/landing-pages/products/voicebiometrics/

- ¿Cuántos inicios de intentos de acceso se han producido que luego se han abandonado? Esto proporcionaría una idea a la organización de cuantos usuarios deciden no acceder a la aplicación precisamente por utilizar certificados o que por problemas de complejidad de uso del certificado por parte de los usuarios, han decidido abandonar el acceso.

4.3 Sistema de gestión de contraseñas

4.3.1 Definición ISO

Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.

4.3.2 Guía de implementación ISO

Un sistema de gestión de contraseñas debe:

- Imponer el uso de identificadores de usuario y contraseñas individuales para mantener la trazabilidad.
- Permitir a los usuarios elegir y cambiar sus propias contraseñas e incluir un procedimiento de confirmación de ésta para evitar errores durante su selección.
- Imponer alternativas para la calidad de las contraseñas.
- Obligar a los usuarios a cambiar sus contraseñas tras el primer inicio de sesión.
- Obligar a cambios periódicos de contraseñas y siempre que se necesite.
- Mantener un registro de las últimas contraseñas utilizadas y prevenir su reutilización (histórico de contraseñas).
- No mostrar las contraseñas en la pantalla mientras se escriben.
- Guardar la información sobre contraseñas separada de los datos de los sistemas de aplicación.
- Proteger cómo se guardan y transmiten las contraseñas.

En ocasiones, la elección de la contraseña no se deja al usuario, sino que se utilizan sistemas que generan y entregan una contraseña al usuario que éste no puede cambiar. En esos casos, ciertos requisitos expuestos arriba deben ser obviados.

4.3.3 Riesgos de seguridad

No utilizar sistemas de gestión de contraseñas adecuados debilita todo intento de control del proceso de autenticación y su consecuente acceso, por lo que debilita la confidencialidad, integridad e incluso disponibilidad de la información o servicio accedido.

La trazabilidad en sí no se ve afectada, aunque sí falseada, puesto que la identidad del causante de una determinada acción se puede seguir identificando, pero ésta identificación resultará falsa.

4.3.4 Recomendaciones y Buenas prácticas

En la actualidad, cualquier sistema experto en autenticación de usuarios y también en gestión de identidades proporciona herramientas con amplias posibilidades de configuración y parametrización para proporcionar unos mecanismos de cambio de contraseña adaptables a casi cualquier política o directriz, por lo que las recomendaciones indicadas por el estándar en general siempre se podrán aplicar.

Solamente cuando se utilizan aplicaciones o sistemas muy antiguos, una organización puede verse obligada a simplificar las políticas de contraseñas a exigir. En estos casos, sería muy recomendable que esa aplicación “limitada”, estuviera controlada y robustecida por mecanismos de control alternativos, por ejemplo, un firewall que controle desde qué redes o qué IPs concretas pueden acceder o que se controle la franja horaria en que se puede acceder.

De la lista de recomendaciones ofrecida por el estándar, una de ellas, a día de hora está dejando de ponerse en práctica: “No mostrar las contraseñas en la pantalla mientras se escriben”. Cuando se escribe la contraseña de conexión a una red wifi, es posible visualizar la contraseña.

El motivo se debe a que las contraseñas para redes wifi son largas y complejas y para evitar problemas a los usuarios, se les permite visualizarlas en claro.

También existen aplicaciones y add-ons o extensiones de algunos navegadores que han desarrollado esta propiedad.

Su uso no está recomendado, puesto que expone la seguridad del sistema.

4.3.5 Tecnologías aplicables

Los sistemas expertos de control de acceso y de aprovisionamiento de usuarios que se han visto en otros apartados, proporcionan un sistema de gestión de contraseñas que cumple con las recomendaciones indicadas por el estándar.

En cambio, se ha hecho referencia en el apartado anterior a aplicaciones o extensiones de navegadores que permiten visualizar el campo contraseña de cualquier servicio web. Algunos ejemplos de estas aplicaciones o extensiones son:

- Showpassword, de Scalabium Software[47]
- Showpassword, para Mozilla Firefox[48]

4.3.6 Métricas para el cuadro de mando

Cuando una organización utilice un sistema de gestión de contraseñas, es interesante obtener información que permita conocer el acierto o no de sus usuarios con sus contraseñas. Esto proporciona a una organización un indicador sobre la madurez que tienen sus usuarios en el uso de contraseñas.

- ✓ ¿Cuántos usuarios tuvieron que corregir/completar su contraseña antes de indicar una que cumpliera todos los criterios exigidos? ¿Cuántos usuarios no tuvieron que hacerlo para un mismo período de tiempo?
- ✓ ¿Cuántos usuarios han tratado de reutilizar contraseñas? ¿Cuántos usuarios no tuvieron que hacerlo para un mismo período de tiempo?
- ✓ ¿Cuántos usuarios han cambiado su contraseña una vez caducada y cuántos lo hacen con antelación a que caduque? ¿con cuánta antelación?

4.4 Utilización de programas o utilidades privilegiadas

4.4.1 Definición ISO

Se debe restringir y controlar estrechamente el uso de utilidades que pueden ser capaces de anular los controles de aplicaciones y sistemas.

4.4.2 Guía de implementación ISO

Se deben contemplar las siguientes recomendaciones cuando se utilicen utilidades privilegiadas (que la mayoría de los sistemas tienen):

- Aplicar procedimientos de identificación, autenticación y autorización para el uso de este tipo de utilidades.

[47] http://www.scalabium.com/showpw.htm

[48] https://addons.mozilla.org/en-US/firefox/addon/show-password/

- Segregar este tipo de utilidades del resto de aplicaciones software.
- Limitar el uso de este tipo de utilidades al número mínimo, práctico y necesario de usuarios en los que se confía y que tendrán autorización.
- Tener autorización expresa para el uso de este tipo de utilidades.
- Limitar la disponibilidad de este tipo de utilidades, por ejemplo, sólo durante la realización de un cambio autorizado.
- Registrar en logs todo uso que se haga de este tipo de utilidades.
- Definir y documentar niveles de autorización sobre este tipo de utilidades.
- Eliminar o al menos deshabilitar toda utilidad innecesaria.
- Evitar que las utilidades estén disponibles para los usuarios cuando tiene acceso a aplicaciones en sistemas en los que se requiera segregación de tareas.

4.4.3 Riesgos de seguridad

Disponer de acceso a las utilidades privilegiadas de los sistemas permite no solo acceder, modificar o borrar información, sino además cambiar el comportamiento o los procesos sobre ésta y más importante, permite ocultar las acciones realizadas, ya que se tiene privilegios para desactivar medidas de seguridad, medidas de auditoría y medidas de rastreo.

Atenta contra todas las dimensiones de la seguridad: la confidencialidad, la integridad, la disponibilidad y la trazabilidad.

4.4.4 Recomendaciones y Buenas prácticas

La primera y casi más importante recomendación sería tener identificadas todas las utilidades privilegiadas de las aplicaciones y sistemas. Sin su adecuada identificación no se puede prevenir un uso indebido de las mismas.

En general, los sistemas operativos vienen dotados con multitud de servicios, protocolos, aplicaciones y utilidades. Es una buena costumbre, desinstalar, o al menos, deshabilitar todos aquellos que no vayan a ser utilizados, puesto que posibles vulnerabilidades de éstos pueden llegar a facilitar una entrada de acceso a un sistema. Precisamente por no ser utilizados, se descuida su protección.

Igual que a las aplicaciones se les ha exigido la existencia de un control de acceso que limite la exposición de la información que gestionan, con las aplicaciones, herramientas o utilidades privilegiadas la exigencia es aún mayor, especialmente cuando se trata de entornos de Producción.

Una forma común de controlar estos accesos es considerar las cuentas de usuarios privilegiados como cuentas a utilizar únicamente en caso de incidencias, creando para su uso un flujo formal de petición, autorización y entrega temporal de usuario:

> Una vez que una aplicación o servicio está funcionando, acceder a alguna utilidad privilegiada a cualquier nivel de la aplicación sólo estará justificado por una necesidad de solventar algún tipo de incidente o por una actualización. En algunas organizaciones, las cuentas de usuarios privilegiados son conocidas únicamente por ciertas personas que no son quienes operan ni administran. En caso de que un operador o administrador necesite accede, utiliza algún flujo formal de petición del usuario de incidencias, que sin aprobación formal no se le entregará. Habitualmente además, esta entrega de usuario es un período de tiempo limitado y estimado en la petición, por ejemplo dos horas. Al transcurso de ese tiempo, se fuerza un cambio de contraseña y se cierra la sesión. El usuario de incidencias vuelve a quedar a salvo.

Otra forma común de controlar estos accesos es haciendo uso de sistemas de control de acceso específicos para entornos administrativos:

> El sistema de control de acceso experto es el punto de acceso de todo operador o administrador. Éste tiene en el sistema experto su propio usuario y contraseña personal. Para acceder a utilizar cualquier utilidad privilegiada, el usuario tiene primero que autenticarse ante el sistema experto y en función de los privilegios identificados para el usuario, el propio sistema experto establecerá la conexión entre el usuario y el sistema o utilidad final a administrar. En ningún momento el usuario llega a conocer la cuenta y contraseña con la que se conectó al sistema final. El sistema experto realizó esta tarea como intermediario que es.

El tamaño de una organización, o más de bien en función del volumen de sistemas que una organización tenga, es recomendable el uso del primer o del segundo modelo de control explicado. Es sencillo verlo con un ejemplo:

- Una organización con pocos sistemas, tendrá uno o un par de administradores que todas las máquinas y aplicaciones. En general, es una situación acotada y relativamente fácil de controlar. La solución basada en un flujo de petición es suficiente y aceptable.
- En una organización algo mayor, puede ser que ya haya, por ejemplo 10 administradores, que mantengan un total de 50 máquinas con servidores web, de aplicaciones, de bases de datos, de documentación, de correo electrónico…. Quizás, el modelo de flujos todavía pueda seguir siendo válido, y que el flujo de petición, autorización siga siendo aceptable y eficiente.
- Pero en una organización media o grande, este tipo de flujos podrían ser ineficientes, bloqueando o retrasando cualquier acción administrativa. Ya no se habla de 10 administradores para todo, sino de un equipo de profesionales que administran por ejemplo desde un CPD cientos y miles de servidores con cientos y

miles de servicios. El volumen de usuarios privilegiados sería incontrolable sin el uso de este tipo de herramientas expertas.

4.4.5 Tecnologías aplicables

Para el primer modelo descrito, sería suficiente con cualquiera de las herramientas de ticketing que se han indicado en apartados anteriores de este documento.

En cambio para el segundo modelo, un ejemplo de este tipo de sistemas expertos sería:

- IBM Security Privileged Identity Manager[49]
- CyberArk Privileged Session Manager[50]

4.4.6 Métricas para el cuadro de mando

Una métrica importante en este apartado sería:

- ✓ Identificar cuántos sistemas/herramientas o utilidades privilegiadas todavía están sin un control sobre su cuenta de usuario privilegiada.

Esto permitiría conocer el grado de penetración que el control tiene en una organización.

Por otro lado, y concentrando el foco en donde sí se aplica el control, las métricas deberían obtener información que permita a la organización estimar si se hace un uso adecuado de las cuentas privilegiadas o un sobre-uso, es decir, un uso exagerado en cuyo caso debería analizarse las causas, como simplemente deficiencias técnicas para administrar, o quizás una mala segregación de funciones. Algunas métricas que podrían ayudar a obtener estos indicadores de uso adecuado sería:

- ✓ Número de accesos privilegiados a cada sistema por semana, y/o por mes.
- ✓ Porcentaje de accesos privilegiados que son realizados de manera casi consecutiva a un mismo sistema (por ejemplo en un margen de tiempo de 1 hora).

[49] http://www-03.ibm.com/software/products/es/pim

[50] http://www.cyberark.com/products/privileged-account-security-solution/privileged-session-manager/

4.5 Control de acceso al código fuente de programas

4.5.1 Definición ISO

Se debe restringir el acceso al código fuente de los programas.

4.5.2 Guía de implementación ISO

Se debe controlar estrictamente el acceso al código fuente de cualquier programa así como a cualquier ítem asociado a ello (como diseños, especificaciones, planes de verificación y/o planes de validación) con objeto de:

- prevenir la incorporación de funcionalidades no autorizadas,
- evitar cambios no intencionados, y
- mantener la confidencialidad de la propiedad intelectual.

Este control se puede aplicar mediante el uso de sistemas de bibliotecas que almacenan de manera centralizada y controlada los códigos fuente de aplicaciones y programas. Se deben tener en cuenta las siguientes recomendaciones cuando se utilicen tales bibliotecas con objeto de reducir los posibles riesgos de corrupción de los programas:

- Cuando sea posible, por su seguridad, las bibliotecas con los códigos fuente no deben estar guardadas en sistemas (entornos) que sean operacionales.
- Tanto el código fuente como las bibliotecas que los almacenan deben gestionarse de acuerdo con procedimientos establecidos.
- El personal de soporte no debe tener acceso ilimitado a las bibliotecas de códigos fuente.
- La actualización de bibliotecas de códigos fuente y de su documentación asociada y el proporcionar los códigos fuente a los programadores sólo debe hacerse tras una apropiada autorización a ello.
- Los listados de programas deben permanecer en entornos seguros.
- Se debe mantener un log de auditoría de todos los accesos que se realicen a las bibliotecas de códigos fuente.
- El mantenimiento y la copia de bibliotecas de códigos fuente debe estar sujeto a estrictos procedimientos de control de cambios, como recomiendan otros dominios del estándar.
- Si se tuviera intención de publicar el código fuente de una aplicación, se debería considerar la aplicación de controles adicionales que permitan garantizar su integridad, como las firmas digitales.

4.5.3 Riesgos de seguridad

El acceso inapropiado al código fuente puede provocar graves riesgos, desde permitir conocer el funcionamiento interno de aplicaciones y sistemas y por tanto la identificación de vulnerabilidades para futura explotación de las mismas hasta modificaciones del código para forzar la ejecución de comportamientos no deseados de las mismas o permitir accesos no autorizados.

Esto puede provocar riesgos en la confidencialidad, la integridad y la disponibilidad en primer lugar, pero también puede afectar a la trazabilidad de acciones sobre la aplicación.

4.5.4 Recomendaciones y Buenas prácticas

Los controles sobre el código fuente vienen principalmente impuestas por la necesidad de control de que los programadores trabajen siempre sobre últimas versiones, facilitar la integración de módulos que han hecho diferentes programadores, garantizar trazabilidad histórica de los cambios y garantizar vuelta atrás de las nuevas versiones o modificaciones que se realizan. Es decir, hacen un control sobre las versiones desarrolladas.

Históricamente este ha sido el sentido de las aplicaciones de control de versiones a las que se le añadieron después los controles de seguridad.

Este tipo de aplicaciones funcionan como un repositorio o sistema de ficheros. Almacenan en carpetas y subcarpetas ficheros con las nuevas versiones de código fuente desarrolladas o más bien con las diferencias entre dos versiones para minimizar la necesidad de espacio requerido. El control de acceso es imprescindible en este entorno que guarda información tan variante y dinámica y el uso de cuentas de usuario personales y no compartidas imprescindible.

4.5.5 Tecnologías aplicables

Son dos los sistemas de control de versiones más conocidos y más utilizados entre la comunidad y proyectos de desarrollo libres pero también de ámbito empresarial:

- Subversion[51] también conocido como SVN.
- Eclipse[52]. Inicialmente desarrollado por IBM pero posteriormente fue continuado por la Fundación Eclipse como software libre.

[51] http://subversion.apache.org/

[52] http://www.eclipse.org/home/

4.5.6 Métricas para el cuadro de mando

En el contexto de la seguridad las métricas irían orientadas a identificar posibles accesos fraudulentos o malos usos:

- ✓ Número de accesos concurrentes con un mismo usuario, lo que proporcionaría una idea del volumen de usuarios que se comparten.
- ✓ Intentos de acceso fallidos consecutivos que se producen.

CUADRO DE MANDOS

1. Introducción

A lo largo del proyecto, en cada control de seguridad, se han ido identificando diferentes métricas que permiten obtener información concreta sobre el estado de implantación del control en particular.

La necesidad de utilización de unas u otras métricas en realidad es cuestión de cada organización y del objetivo de seguridad que quiera monitorizar. Lo habitual es que los cuadros de mando sean una herramienta, utilizada en general por la Dirección o Gerencia de una organización, que les facilite información en los términos y con el tipo de lenguaje que la Dirección o Gerencia utilizan con el objetivo de poder tomar decisiones.

Por tanto, aunque un cuadro de mandos podría proporcionar información sobre el número de reseteos de contraseñas que se han realizado por ejemplo en el último mes, lo normal es que el cuadro de mandos se utilice para algo más que mostrar números a modo de tabla, sino que sirva para mostrar una evolución en el comportamiento de los usuarios, una tendencia de mejora o empeoramiento de un comportamiento, el grado de avance o de efectividad de una solución implantada, etc. Es decir, para mostrar resultados de negocio.

El estándar ISO/IEC 27004 define un proceso para el diseño de métricas y mediciones de seguridad, en el marco de un sistema de gestión de seguridad de la información.

Este proyecto no tiene por objetivo la implementación completa del estándar, pero sí se apoya en él para mostrar un ejemplo de un cuadro de mandos de seguridad.

Por tanto, en los siguientes apartados de este documento se recogerá el amplio conjunto de métricas que se han ido identificando de manera específica para cada control, se definirán las mediciones del cuadro de mandos siguiendo las fichas o plantillas que sugiere el estándar para garantizar que se realiza un análisis detallado de la medición deseada y se plasmarán finalmente en un cuadro de mandos, para el que se ha utilizado una versión de prueba de una conocida aplicación de cuadros: SAP BusinessObjects Dashboards[53].

[53] http://www.sap.com/pc/analytics/business-intelligence/software/dashboards/index.html

2. Métricas de seguridad

A lo largo del documento, en cada control se han ido identificando métricas que podían resultar interesantes de extraer. Algunas de esas métricas pueden proporcionar una idea del grado de implantación del estándar de seguridad dentro de una organización, y otras proporcionar información importante por ejemplo para un responsable de seguridad que vela por no sufrir ataques de seguridad o para un responsable de un servicio de Atención al usuario, que necesita contabilizar el número de llamadas para reseteo de contraseñas recibidas.

El cuadro de mandos que se ha seleccionado para este proyecto ha sido el de un cuadro de mandos bajo las siguientes suposiciones:

- Irá dirigido a la Dirección de una organización, de tamaño mediano-pequeño,
- que decidió alinearse, hace algunos años, al estándar de seguridad como garante de la aplicación de medidas de seguridad, y así
- apoyar el que sus clientes puedan seguir "confiando" en la compañía y en los servicios que ofrece.

Las siguientes tablas mostrarán el conjunto de métricas identificadas en cada control a lo largo de este documento. Aparecerán resaltadas con un recuadro de chequeo marcado (☑) aquellas métricas concretas que posteriormente se empleen para elaborar el cuadro de mandos para la Dirección.

Tabla 1. Conjunto de métricas para el objetivo Requisitos de Negocio para el control de accesos

REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS	
Política de control de accesos	
☑	¿Existe una política definida y escrita que estipule cómo y de qué forma se puede acceder a las aplicaciones y sistemas de la organización?
☑	¿Cada cuánto tiempo se revisa esta política? Anualmente, bianualmente, más, nunca…
☑	¿Existen aplicaciones de negocio que no se vean afectadas por esta política, es decir, que queden fuera del ámbito de aplicación de la política? ¿Cuántas (%), con respecto al número total de aplicaciones de negocio existentes en la organización?
☑	¿En cuántos sistemas ya se ha implantado la política? ¿Qué porcentaje representa respecto del total de los sistemas alcanzados por la política?
☑	¿Cuántas deficiencias o no cumplimientos se han identificado en un período de revisión (para un sistema en concreto, o para un área o departamento, o para la organización en su totalidad? ¿ha aumentado o disminuido respecto a no cumplimientos obtenidos de revisiones anteriores?
Acceso a Redes y Servicios	

☑	¿Existe una política definida y escrita que estipule cómo y de qué forma se puede acceder a las redes y servicios de la organización?
☑	¿Contempla la política la existencia de una segmentación de redes y define quiénes pueden tener acceso a cada segmento?
☑	¿Contempla la política diferenciar entre los diferentes medios de acceso y establece controles sobre ellos?
☑	¿Cada cuánto tiempo se revisa esta política? Anualmente, bianualmente, más, nunca…

Tabla 2. Conjunto de métricas para el objetivo Gestión de acceso de usuarios

GESTIÓN DE ACCESO DE USUARIOS
Registro y des-registro de usuarios
¿Existe un proceso formal para solicitar el registro y des-registro en la Organización?
¿Existe una aplicación o herramienta en la que se gestionen automáticamente las peticiones de registro y des-registro?
¿Cuántas aplicaciones y sistemas disponen de un proceso formal para el registro y el des-registro y que utilizan la herramienta de peticiones? ¿Qué porcentaje supone respecto del total existente en la organización?
¿Cuántas aplicaciones y sistemas disponen de un proceso formal para el registro y el des-registro, pero que no utilizan la herramienta de peticiones? ¿Qué porcentaje supone respecto del total existente en la organización?
¿Cuántas aplicaciones y sistemas no disponen de ningún proceso formal y por tanto quedan fuera del control de la organización?
¿Cuántas peticiones son de registro y cuántas de des-registro?
¿Cuál es el tiempo medio de resolución de una petición de registro o des-registro?
¿Cuántas peticiones están en espera de ser validadas en un instante determinado y cuánto tiempo llevan esperando?
Aprovisionamiento del acceso de usuarios
¿Existe un proceso formal para solicitar el acceso y la cancelación de acceso a las aplicaciones y sistemas de una organización?
¿Existe una aplicación o herramienta en la que se gestionen automáticamente este tipo de peticiones?
¿Cuántas aplicaciones y sistemas se apoyan en la herramienta de gestión automatizada? ¿Qué porcentaje supone respecto del total existente en la organización?
¿Cuántas aplicaciones y sistemas no utilizan la herramienta de gestión automatizada? ¿Qué porcentaje supone respecto del total existente en la organización?
¿En cuántas aplicaciones y sistemas no disponen ni siquiera de un proceso formal y por tanto quedan fuera del control de la organización?
¿De cuántos identificadores de usuario diferentes requiere un empleado de una organización?
Peticiones de acceso:
¿Cuántas peticiones de acceso se reciben?

¿Cuál es el tiempo medio de resolución de una petición de acceso?
¿Cuántas peticiones están en espera de ser validadas en un instante determinado y cuánto tiempo llevan esperando?
¿Cuántas peticiones han sido rechazadas y por qué motivos?
¿Cuántas de las peticiones se deben a cambios en el perfil, rol o puesto que desempeña un usuario?
Peticiones de cancelación de acceso:
¿Cuántas peticiones cancelación de acceso se reciben?
¿Cuál es el tiempo medio de resolución de una petición cancelación de acceso?
¿Cuántas se deben a baja en la organización?
Gestión de los derechos de acceso privilegiados
¿Cuántos usuarios privilegiados "personales" existen en el sistema? ¿Qué porcentaje representa respecto del total de usuarios privilegiados "genéricos" del sistema (es decir, usuarios privilegiados que no están directamente asociados a una persona, propietaria del usuario)?
¿Cuántos accesos se realizan con el usuario o usuarios privilegiados (accesos diarios y también acumulados mensuales para cálculo de media de uso)?
¿Qué tipo de acciones se realizan (cuando sea posible identificarlo)?
¿Cuántos intentos de acceso fallidos de usuarios privilegiados se han producido?
Gestión de la información de autenticación secreta de los usuarios
¿Cuántas solicitudes de regeneración de contraseñas por olvido se han recibido?
¿Cuántas de esas solicitudes se han detectado que fueran fraudulentas o maliciosas?
¿Cuántas solicitudes de desbloqueo de contraseñas o cuentas se han recibido?
¿Cuántas de esas solicitudes se han detectado que fueran fraudulentas o maliciosas?
Revisión periódica de los derechos de acceso de los usuarios
¿Se realizan procesos de revisión periódicos?
¿Cuántas cuentas obsoletas se han identificado y qué porcentaje supone respecto del total de cuentas existente?
¿Cuántas cuentas sin propietario se han identificado y qué porcentaje supone respecto del total de cuentas existente?
¿Cuántas cuentas con exceso de privilegios se han identificado y qué porcentaje supone respecto del total de cuentas existente?
Crecimiento o decrecimiento de las métricas anteriores respecto a periodos de revisión anteriores.
Eliminación o ajuste de derechos de acceso
¿Existe un proceso formal para solicitar el acceso y la cancelación de acceso a las aplicaciones y sistemas de una organización?
¿Existe una aplicación o herramienta en la que se gestionen automáticamente este tipo de peticiones?
¿Cuántas aplicaciones y sistemas se apoyan en la herramienta de gestión automatizada? ¿Qué porcentaje supone respecto del total existente en la organización?
¿Cuántas aplicaciones y sistemas no utilizan la herramienta de gestión automatizada? ¿Qué

porcentaje supone respecto del total existente en la organización?
¿En cuántas aplicaciones y sistemas no disponen ni siquiera de un proceso formal y por tanto quedan fuera del control de la organización?
¿De cuántos identificadores de usuario diferentes requiere un empleado de una organización?
Peticiones de acceso:
¿Cuántas peticiones de acceso se reciben?
¿Cuál es el tiempo medio de resolución de una petición de acceso?
¿Cuántas peticiones están en espera de ser validadas en un instante determinado y cuánto tiempo llevan esperando?
¿Cuántas peticiones han sido rechazadas y por qué motivos?
¿Cuántas de las peticiones se deben a cambios en el perfil, rol o puesto que desempeña un usuario?
Peticiones de cancelación de acceso:
¿Cuántas peticiones cancelación de acceso se reciben?
¿Cuál es el tiempo medio de resolución de una petición cancelación de acceso?
¿Cuántas se deben a baja en la organización?

Tabla 3. Conjunto de métricas para el objetivo Responsabilidades de los usuarios

RESPONSABILIDADES DE LOS USUARIOS
Uso de información de autenticación secreta
¿Cuántos intentos de autenticación fallidos se han producido? (para ciertas aplicaciones o sistemas que la organización considere críticos o importantes para analizar).
¿Cuántos bloqueos de cuenta por exceder el número de intentos de autenticación fallidos consecutivos permitidos se han producido? (para ciertas aplicaciones o sistemas que la organización considere críticos o importantes para analizar).
¿Cuántas solicitudes de regeneración de contraseñas por olvido se han recibido?
¿Cuántas de esas solicitudes se han detectado que fueran fraudulentas o maliciosas?
¿Cuántas solicitudes de desbloqueo de contraseñas o cuentas se han recibido?
¿Cuántas de esas solicitudes se han detectado que fueran fraudulentas o maliciosas?

Tabla 4. Conjunto de métricas para el objetivo Control de acceso a sistemas y aplicaciones

CONTROL DE ACCESO A SISTEMAS Y APLICACIONES
Restricción de acceso a la información
¿Cuántas denegaciones de acceso se han producido por no disponer de autorización en la aplicación o sistema?
¿Cuántos intentos de acceso a información, funcionalidades, menús o pantallas correspondientes a perfiles o privilegios mayores que los que tuviera el usuario se han realizado?

Procedimientos de log-on seguro
¿En cuántos sistemas de la organización el proceso de logon cumple las directrices del estándar? ¿qué porcentaje supone respecto al total?
¿En cuántos sistemas de la organización el proceso de logon no cumple las directrices del estándar? ¿qué porcentaje supone respecto al total?
¿Cuántos sistemas de la organización están pendientes de evaluar?
Sistema de gestión de contraseñas
¿Cuántos usuarios tuvieron que corregir/completar su contraseña antes de indicar una que cumpliera todos los criterios exigidos? ¿Cuántos usuarios no tuvieron que hacerlo para un mismo período de tiempo?
¿Cuántos usuarios han tratado de reutilizar contraseñas? ¿Cuántos usuarios no tuvieron que hacerlo para un mismo período de tiempo?
¿Cuántos usuarios han cambiado su contraseña una vez caducada y cuántos lo hacen con antelación a que caduque? ¿con cuánta antelación?
Utilización de programas o utilidades privilegiadas
Identificar cuántos sistemas/herramientas o utilidades privilegiadas todavía están sin un control sobre su cuenta de usuario privilegiada
Número de accesos privilegiados a cada sistema por semana, y/o por mes.
Porcentaje de accesos privilegiados que son realizados de manera casi consecutiva a un mismo sistema (por ejemplo en un margen de tiempo de 1 hora).
Control de acceso al código fuente de programas
Número de accesos concurrentes con un mismo usuario, lo que proporcionaría una idea del volumen de usuarios que se comparten.
Intentos de acceso fallidos consecutivos que se producen

3. Indicadores

El estándar ISO/IEC 27004 proporciona una plantilla con todos los datos que considera necesarios que se recojan y preparen para cuando se está diseñando un cuadro de mandos.

En particular, para este cuadro de mandos se ha seleccionado que muestre qué evolución ha sufrido la organización en cuanto al nivel de madurez de la implantación de la política de control de accesos.

La organización decidió estimar el grado de madurez de la siguiente manera:

Fórmula para calcular el indicador: a * (b+c+d+e).

Lo que responde a las siguientes métricas y varemos:

a) **Existencia de política:**

Sí, 1 punto.

No, 0 puntos.

b) **Existencia de revisiones de la política:**

Sí, al menos bianual, 30 puntos.

Sí, pero cada más de dos años, 0 puntos.

c) **Volumen de aplicaciones a las que alcanza la política:**

Más del 90% de las aplicaciones de la organización, 30 puntos.

Entre el 71% y 90%, 20 puntos.

Entre 51% y 70%, 10 puntos.

Hasta 50%, 0 puntos.

d) **Volumen de aplicaciones en las que está implantada la política:**

Más del 90% de las aplicaciones de la organización, 30 puntos.

Entre el 71% y 90%, 20 puntos.

Entre 51% y 70%, 10 puntos.

Hasta 50%, 0 puntos.

e) **Volumen deficiencias encontradas entre auditorias:**

Menos de un 10% de no conformidades, 0 puntos.

Entre 30% y 10% de no conformidades, 10 puntos.

Más de 30% o que no ha habido auditoría previas con las que comparar, -10 puntos.

El modelo analítico en el que se basará el indicador tras el cálculo de la fórmula es de la siguiente manera:

- **Excelencia de implantación**: Valores entre 80 (1 * (30 + 30 + 30 - 10) implicando mucho implantado, con procesos de revisión frecuentes y se perdona que tengan muchas no conformidades) y 100 (1 * (30 + 30 +30 +10) implicando que además tiene muy pocas no conformidades).

  En el cuadro de mandos se representará con color verde.

- **Implantación buena**: Valores entre 50 (1 * (0 + 20 + 20 +10) implicando que tiene un alcance medio, por lo que están en el buen camino pero se tiene que mejorar) y menos de 80.

  En el cuadro de mandos se representará con color amarillo.

- **Implantación baja**: Valores entre 10 (1*(0 + 10 + 10 -10) implicando que se está simplemente empezando) y menos de 50.

  En el cuadro de mandos se representará con color naranja.

- **Implantación NULA**. Alerta. Valor menor de 10 o sin política (0 * (0 + 0 + 0 + 0))

  En el cuadro de mandos se representará con color rojo.

Siguiendo la plantilla que propone el estándar ISO/IEC 27004, el indicador se documenta en la siguiente tabla:

Tabla 5. Tabla para identificación del constructor de la medición

Identificación del constructor de medición	
Nombre del Constructor de la Medición	Madurez implantación política de control de accesos
Identificador Numérico	Med-01
Propósito del Constructor de la Medición	Mostrar qué evolución ha sufrido la organización en cuanto al nivel de madurez de la implantación de la política de control de accesos
Control/Proceso Objetivo	SGSI
Control(1)/Proceso(1)	SGSI
Control(2)/Proceso(2)	Control y Calidad SGSI
Objeto de medición y atributos	
Objeto de Medición	Resultados del proceso de análisis de riesgos y SGSI de la organización.
Atributos	• Aplicación adaptada a la política de control de accesos de la organización.

	• Volumen de no cumplimientos detectados en auditorías de cumplimiento por aplicación.
Especificación de la medida A	
Medida Base A)	Existencia de política de control de accesos
Método de Medición	Se confirmará existencia de política mediante consulta a Responsables de Seguridad de la organización.
Tipo de Método de Medición	Subjetiva
Escala	Valores de Sí o No
Tipo de Escala	Nominal
Unidad de Medida	Existencia de política
Especificación de la medida B	
Medida Base B)	Existencia de revisiones de la política
Método de Medición	Se confirmará existencia de revisiones de la política mediante consulta a Responsables de Seguridad de la organización.
Tipo de Método de Medición	Subjetiva
Escala	Valores de Sí o No
Tipo de Escala	Nominal
Unidad de Medida	Existencia de revisiones
Especificación de la medida C	
Medida Base C)	Volumen de aplicaciones a las que alcanza la política
Método de Medición	Se obtendrá alcance de aplicación de la política mediante consulta a Responsables de Seguridad de la organización. Se obtendrá número total de aplicaciones existentes en la organización mediante consulta al Director de Informática de la organización. Se obtendrá después el porcentaje que suponen las alcanzadas por la política de control de accesos, respecto del total de aplicaciones existentes en la organización.
Tipo de Método de Medición	Objetivo
Escala	Porcentaje
Tipo de Escala	Ordinal
Unidad de Medida	Sistemas
Especificación de la medida D	
Medida Base D)	Volumen de sistemas o aplicaciones de la organización que ya han adoptado la política de control de accesos.
Método de Medición	Se consultará el número de aplicaciones/sistemas que indican True al atributo "Aplicación adaptada a la política de control de accesos de la

	organización” en los informes de resultados de auditorías. Se obtendrá después el porcentaje que suponen calculando la relación respecto de la medición C).
Tipo de Método de Medición	Objetivo
Escala	Porcentaje
Tipo de Escala	Ordinal
Unidad de Medida	Sistemas
Especificación de la medida E	
Medida Base E)	Volumen de no cumplimientos detectados en auditorías.
Método de Medición	Se consultará en los informes de resultados de las auditorías, el número de no cumplimientos recogidos en el campo “Volumen de no cumplimientos”. Se consultará en los informes de resultados de las auditorías, el número total de requisitos auditados en el campo “Número total requisitos”. Se obtendrá después el porcentaje que suponen los no cumplimientos respecto del total de requisitos auditados.
Tipo de Método de Medición	Objetivo
Escala	Porcentaje
Tipo de Escala	Ordinal
Unidad de Medida	No cumplimientos
Especificación de la medida derivada	
Medida derivada	Transformación de los valores de volúmenes a pesos.

Medición de la función	En función de los valores de volúmenes obtenidos, se asignarán puntos a cada medida a), b), c), d) y e) de la siguiente manera:
	• Existencia de política:
	  ○ Sí, 1 punto.
	  ○ No, 0 puntos.
	• Existencia de revisiones de la política:
	  ○ Sí, al menos bianual, 30 puntos.
	  ○ Sí, pero cada más de dos años, 0 puntos.
	• Volumen de aplicaciones a las que alcanza la política:
	  ○ Más del 90% de las aplicaciones de la organización, 30 puntos.
	  ○ Entre el 71% y 90%, 20 puntos.
	  ○ Entre 51% y 70%, 10 puntos.
	  ○ Hasta 50%, 0 puntos.

	• Volumen de aplicaciones en las que está implantada la política:
	  ○ Más del 90% de las aplicaciones de la organización, 30 puntos.
	  ○ Entre el 71% y 90%, 20 puntos.
	  ○ Entre 51% y 70%, 10 puntos.
	  ○ Hasta 50%, 0 puntos.
	• Volumen deficiencias encontradas entre auditorias:
	  ○ Menos de un 10% de no conformidades, 0 puntos.
	  ○ Entre 30% y 10% de no conformidades, 10 puntos.
	  ○ Más de 30% o que no ha habido auditoría previas con las que comparar, -10 puntos.

Especificación del indicador	
Indicador	• Estado de evolución de implantación expresado en base a varemos sobre las medidas derivadas, y • Tendencia respecto a estado de hace dos años.
Modelo analítico	• a * (b+c+d+e) de año actual • a * (b+c+d+e) de hace dos años
Especificación de los criterios de decisión	

Criterios de decisión	• **Excelencia de implantación**: Valores entre 80 (1 * (30 + 30 + 30 - 10) implicando mucho implantado, con procesos de revisión frecuentes y se perdona que tengan muchas no conformidades) y 100 (1 * (30 + 30 +30 +10) implicando que además tiene muy pocas no conformidades).
	  Se representará con **color verde**.
	• **Implantación buena**: Valores entre 50 (1 * (0 + 20 + 20 +10) implicando que tiene un alcance medio, por lo que están en el buen camino pero se tiene que mejorar) y menos de 80.
	  Se representará con **color amarillo**.
	• **Implantación baja**: Valores entre 10 (1*(0 + 10 + 10 -10) implicando que se está simplemente empezando) y menos de 50.
	  Se representará con **color naranja**.
	• **Implantación NULA**: Alerta. Valor menor de 10 o sin política (0 * (0 + 0 + 0 + 0))
	  Se representará con **color rojo**.
	
	Además, se mostrará resultado actual y resultado del período anterior para su comparación.

Resultados de las mediciones	
Interpretación del indicador	• **Verde**: La organización ha cumplido sus objetivos, la implantación de la política de control de acceso está prácticamente implantada en todos los sistemas y aplicaciones. El indicador en futuras revisiones servirá para indicar que no se degrada su cumplimiento. • **Amarillo**: El proceso de implantación de la política de control de accesos está muy avanzado aunque queda trabajo. Sólo si el avance entre período anterior y el actual es escaso, será motivo de alarma para la organización. • **Naranja**: El proceso de implantación tiene un avance muy pequeño. Será especialmente importante analizar el grado de avance entre el período anterior y el actual. Si el avance es pequeño, será motivo de alarma para la organización. • **Rojo**: Alerta. O no se ha iniciado el proceso de implantación o su avance ha sido mínimo. La organización debe solicitar explicaciones y justificaciones para decidir siguientes pasos.
Formato de los informes	Gráfico tipo velocímetro, con franjas de colores en el siguiente orden de peor o mejor resultado: Rojo, Naranja, Amarillo, Verde.
Las partes interesadas	
Cliente para la Medición	La Alta Dirección de la organización
Revisor para la Medición	La Alta Dirección de la organización
Propietario de la Información	El Director de Informática de la organización
Colector de la Información	El Responsable de Seguridad, dentro de la unidad de Informática de la organización
Comunicador de la Información	El Director de Informática de la organización
Frecuencia/Periodo	
Frecuencia de la Recogida de Datos	Cada 6 meses
Frecuencia del Análisis de Datos	Cada año
Frecuencia de los Informes con Resultados de las Mediciones	Bianual
Revisión de la Medición	Revisión bianual
Periodo de Medición	Bianual

4. Extracción de datos. Cálculo de mediciones

Con las mediciones definidas y los indicadores diseñados, la organización ya puede periódicamente realizar una revisión, obtener información que resuelva sobre las métricas utilizadas y obtener así los valores de los indicadores.

En la siguiente tabla se muestra los datos que la organización habría obtenido tras la revisión actual junto con los datos que se obtuvieron hace dos años. La existencia de ambos datos son necesarios para poder realizar la comparación y así conocer la evolución sufrida en la organización:

Tabla 6. Tabla con resultados de las métricas

	A	B	D
1		**Año 2013**	**Año 2015**
2	**Existencia política**	SI	SI
3	**Periodicidad revisión**	Bianual	Bianual
4	**Volúmen Aplicaciones afectadas**	95%	95%
5	**Volumen aplicaciones con implantación**	45%	70%
6	**Volúmen deficiencias**	25%	25%
7	**Totales:**	N/A	N/A
8			

Cada uno de esos datos responde después a un peso concreto según el diseño del indicador:

Tabla 7. Tabla con resultados de las métricas y el valor final tras aplicar la fórmula del indicador

	A	B	C	D	E
1		**Año 2013**	**Pond.**	**Año 2015**	**Pond.**
2	**Existencia política**	SI	1	SI	1
3	**Periodicidad revisión**	Bianual	30	Bianual	30
4	**Volúmen Aplicaciones afectadas**	95%	30	95%	30
5	**Volumen aplicaciones con implantación**	45%	5	70%	20
6	**Volúmen deficiencias**	25%	0	25%	0
7	**Totales:**	N/A	**65**	N/A	**80**
8					

Finalmente, una vez que se tienen datos de la revisión realizada en 2015 y datos de la revisión realizada hace dos años (2013), ya se puede ejecutar el cuadro de mandos.

5. Cuadro de mandos

Este sería el cuadro de mandos que se presentaría a la Dirección.

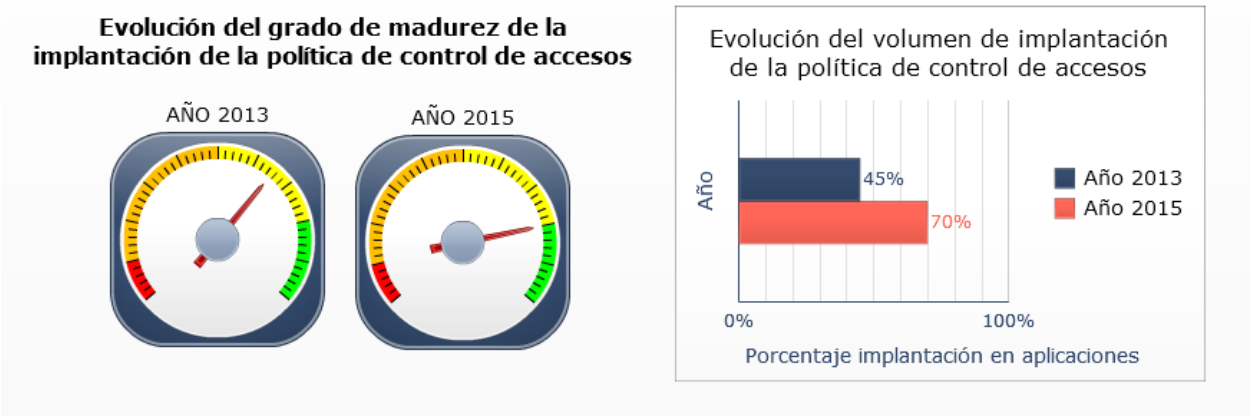


Figura 5. Cuadro de mandos. Evolución del grado de madurez de la implantación de la política de control de accesos en la organización

En el cuadro de mandos se puede fácilmente comparar el grado de madurez que tiene actualmente la organización con respecto al grado de madurez que tenía hace dos años.

Además, el cuadro de mandos aparece acompañado de otro indicador que resalta el grado de avance que ha tenido lugar implantando la política de control de accesos entre las aplicaciones de la organización. Es una forma de justificar ante la Dirección los resultados mostrados.

CONCLUSIONES

1. Conclusiones a la finalización del proyecto

El estudio realizado a lo largo del proyecto ha permitido sacar conclusiones en varios sentidos:

a) Conclusiones respecto a los contenidos de la propia norma:

El proyecto se inició cuando la versión vigente de la norma era la anterior a la del 2013. Aunque en su momento no se desarrolló demasiado, la recuperación del proyecto fin de carrera dos años después y su adecuación a la versión 2013, permitió identificar diferencias entre ambas versiones. La versión del 2013 es una norma mucho más clara y ordenada. La versión del 2005 era una mezcla de recomendaciones a temáticas, no muy ordenada y hasta cierto punto "casual"; por ejemplo, se sugería la aplicación de controles a los dispositivos o temas de moda que se iniciaban en el momento (teletrabajo, limpieza del escritorio y puesto de trabajo….), pero esa definición daba lugar a quedarse obsoleta con facilidad, además de que, precisamente por tratar casuísticas concretas no creo que fomentara precisamente la creación de políticas de control de acceso consistentes.

La versión del 2013 del estándar, es una versión más limpia, más genérica y con menos facilidad de quedarse obsoleta, pero aun así la sigo considerando desordenada. Creo que siguen haciendo una mezcla en los controles para hablar de lo mismo. Algunos ejemplos al respecto (resaltando palabras clave para facilitar entender los galimatías existentes):

- El apartado 9.1 de la norma sugiere mecanismos para control de acceso a la información. Por otro lado, el apartado 9.4 sugiere mecanismos para control de acceso a aplicaciones y sistemas. ¿Por qué entonces el primer punto de este apartado, es decir el apartado 9.4.1, que debería ser referido a aplicaciones y sistemas, habla de restricciones de acceso **a información**? Pero ¿no hablaban ya de la información en el 9.1?
- Otro ejemplo, de nuevo con el primer apartado 9.1. Este apartado se titula Requisitos de negocio para el control de accesos y es donde indican la necesidad de creación de políticas de control de acceso que limiten el acceso a la información. ¿Por qué entonces incluir en el apartado 9.1.2 de Accesos a **redes y servicios de red**? ¿No sería más adecuado que lo asociaran al apartado 9.4 de Accesos a sistemas y aplicaciones?
- Y un último ejemplo de desorden de información está en el apartado 9.2 titulado Gestión de acceso de usuarios.

  Al inicio de dicho apartado se indica la necesidad de procedimientos de registro y de des-registro de usuarios. El apartado continúa después exigiendo la existencia de procedimientos para solicitar o cancelar permisos de acceso. Continúa después haciendo una mención especial al tratamiento de usuarios privilegiados así como a la gestión de las contraseñas de acceso.

Y por último habla de la necesidad de establecer un proceso de revisión que controle que todos los procedimientos anteriores se realizan y se realizan bien y que no se mantienen usuarios obsoletos.

Bien, siendo éste el hilo argumental del apartado, ¿por qué incluir justo al final un último apartado que hable de cambio o eliminación de **permisos de acceso**? En mi opinión hacer perder cualquier idea de guion estructurado; ¿no debería mejor formar parte del apartado de solicitud o cancelación de permisos de acceso, o al menos, justo a continuación de ese apartado?

En definitiva, creo que los contenidos deberían ser más ordenados y esta sería mi sugerencia:

- Necesidad de creación de una política de control de accesos basada en requisitos de negocio. Papel de los propietarios de la información.
- Necesidad de Gestión de usuarios
- Responsabilidades de los usuarios
- Control de acceso a sistemas y aplicaciones
- Control en los mecanismos de acceso, garantizando que se contemplan siempre accesos internos (redes internas) y accesos externos (desde Internet).

b) Independientemente del contenido en sí de la norma, la elaboración del proyecto hace obvia la variedad de formas diferentes en que los controles de seguridad pueden implantarse en las organizaciones.

   Es imprescindible que cada organización analice exactamente qué necesita, qué le importa y qué riesgos y debilidades tiene. Será el mejor mecanismo para que puedan identificar la forma más adecuada de implantar los controles para ellos. Eso sí, sin un proceso de revisión continuo como el definido en ISO/IEC 27001, la implantación podrá ser exitosa inicialmente, pero rápidamente se quedará obsoleta y probablemente ineficiente.

c) Y por último, conclusiones sobre el enriquecimiento personal que ha supuesto el proyecto. El proyecto ha permitido analizar los procedimientos que durante años he ido conociendo en diferentes organizaciones como usuaria de ellos. Los procedimientos de las organizaciones, fuera de contexto, en ocasiones pueden parecer inocuos, sin sentido o incluso molestos para sus usuarios, pero conocer la finalidad de su existencia y la interrelación entre unos y procesos, da sentido a muchas situaciones que los usuarios de sistemas de información se encuentran en su día a día.

La forma en que se ha analizado este dominio de la norma, deja abierto un camino para analizar de la misma manera otros controles y descubrir así su sentido real y práctico cuando se encuentra implementado en una organización

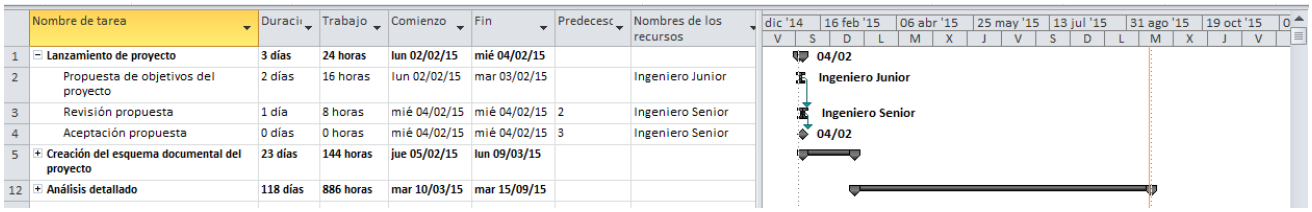
PLANIFICACIÓN Y PRESUPUESTO

1. Planificación

Para abordar el desarrollo del proyecto, se realizaron tres tareas principalmente:

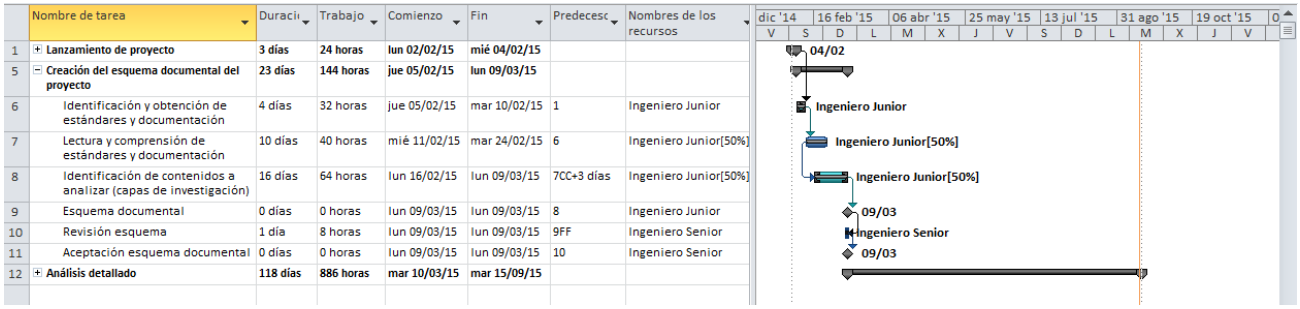
- Una tarea de identificación del proyecto y propuesta al Tutor.
- Una tarea de preparación de un borrador o esqueleto que oriente el trabajo, objetivos y contenidos esperados.
- Y por último el desarrollo propio de los contenidos.

En las siguientes imágenes puede verse el detalle de cada una de las tareas, junto al esfuerzo y recursos dedicados en cada sub-actividad.



	Nombre de tarea	Duraci	Trabajo	Comienzo	Fin	Predecesc	Nombres de los recursos
1	**Lanzamiento de proyecto**	**3 días**	**24 horas**	**lun 02/02/15**	**mié 04/02/15**		
2	Propuesta de objetivos del proyecto	2 días	16 horas	lun 02/02/15	mar 03/02/15		Ingeniero Junior
3	Revisión propuesta	1 día	8 horas	mié 04/02/15	mié 04/02/15	2	Ingeniero Senior
4	Aceptación propuesta	0 días	0 horas	mié 04/02/15	mié 04/02/15	3	Ingeniero Senior
5	**Creación del esquema documental del proyecto**	**23 días**	**144 horas**	**jue 05/02/15**	**lun 09/03/15**		
12	**Análisis detallado**	**118 días**	**886 horas**	**mar 10/03/15**	**mar 15/09/15**		

Figura 6. Detalle de la tarea de Lanzamiento del proyecto



	Nombre de tarea	Duraci	Trabajo	Comienzo	Fin	Predecesc	Nombres de los recursos
1	**Lanzamiento de proyecto**	**3 días**	**24 horas**	**lun 02/02/15**	**mié 04/02/15**		
5	**Creación del esquema documental del proyecto**	**23 días**	**144 horas**	**jue 05/02/15**	**lun 09/03/15**		
6	Identificación y obtención de estándares y documentación	4 días	32 horas	jue 05/02/15	mar 10/02/15	1	Ingeniero Junior
7	Lectura y comprensión de estándares y documentación	10 días	40 horas	mié 11/02/15	mar 24/02/15	6	Ingeniero Junior[50%]
8	Identificación de contenidos a analizar (capas de investigación)	16 días	64 horas	lun 16/02/15	lun 09/03/15	7CC+3 días	Ingeniero Junior[50%]
9	Esquema documental	0 días	0 horas	lun 09/03/15	lun 09/03/15	8	Ingeniero Junior
10	Revisión esquema	1 día	8 horas	lun 09/03/15	lun 09/03/15	9FF	Ingeniero Senior
11	Aceptación esquema documental	0 días	0 horas	lun 09/03/15	lun 09/03/15	10	Ingeniero Senior
12	**Análisis detallado**	**118 días**	**886 horas**	**mar 10/03/15**	**mar 15/09/15**		

Figura 7. Detalle de la tarea de Preparación del esquema y guion del proyecto

	Nombre de tarea	Duraci	Trabajo	Comienzo	Fin	Predecesc	Nombres de los recursos
1	**Lanzamiento de proyecto**	**3 días**	**24 horas**	**lun 02/02/15**	**mié 04/02/15**		
5	**Creación del esquema documental del proyecto**	**23 días**	**144 horas**	**jue 05/02/15**	**lun 09/03/15**		
12	**Análisis detallado**	**118 días**	**886 horas**	**mar 10/03/15**	**mar 15/09/15**		
13	Traducción controles ISO e identificación riesgos seguridad	19 días	152 horas	mar 10/03/15	mié 08/04/15	9	Ingeniero Junior
14	Identificación buenas prácticas	47 días	188 horas	jue 16/04/15	mié 24/06/15	13FC+5 días	Ingeniero Junior[50%]
15	Identificación tecnologías apoyo	47 días	188 horas	jue 16/04/15	mié 24/06/15	13FC+5 días	Ingeniero Junior[50%]
16	Identificación de métricas en controles	20 días	160 horas	jue 25/06/15	mié 22/07/15	14;15	Ingeniero Junior
17	Punto de control. Revisión	2 días	8 horas	jue 23/07/15	vie 24/07/15	16	Ingeniero Senior[50%
18	Cierre buenas prácticas y tecnologías apoyo	8 días	16 horas	lun 27/07/15	mié 05/08/15	17	Ingeniero Junior[25%]
19	Cierre de métricas en controles	8 días	16 horas	lun 27/07/15	mié 05/08/15	17	Ingeniero Junior[25%]
20	Identificación y obtención de herramienta de cuadro de mandos	6 días	12 horas	mié 29/07/15	mié 05/08/15	18FF	Ingeniero Junior[25%]
21	Preparación escenario cuadro de mandos	7 días	14 horas	mar 28/07/15	mié 05/08/15	18FF	Ingeniero Junior[25%]
22	Diseño de cuadro de mandos teórico	7 días	28 horas	jue 06/08/15	mar 01/09/15	21	Ingeniero Junior[50%]
23	Implementación de cuadro de mandos	7 días	28 horas	jue 06/08/15	mar 01/09/15	21	Ingeniero Junior[50%]
24	Punto de control. Revisión	1 día	4 horas	mié 02/09/15	mié 02/09/15	23	Ingeniero Senior[50%
25	Repaso documentación y ajuste a plantillas	7 días	56 horas	jue 03/09/15	vie 11/09/15	24	Ingeniero Junior
26	Documento Proyecto Fin de Carrera	0 días	0 horas	vie 11/09/15	vie 11/09/15	25	Ingeniero Junior
27	Revisión Proyecto Fin de Carrera	2 días	16 horas	lun 14/09/15	mar 15/09/15	26	Ingeniero Senior
28	Aceptación Proyecto Fin de Carrera	0 días	0 horas	mar 15/09/15	mar 15/09/15	27	Ingeniero Senior

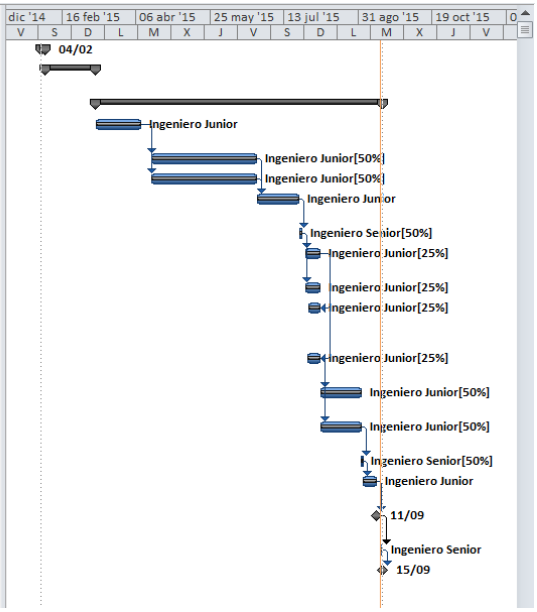
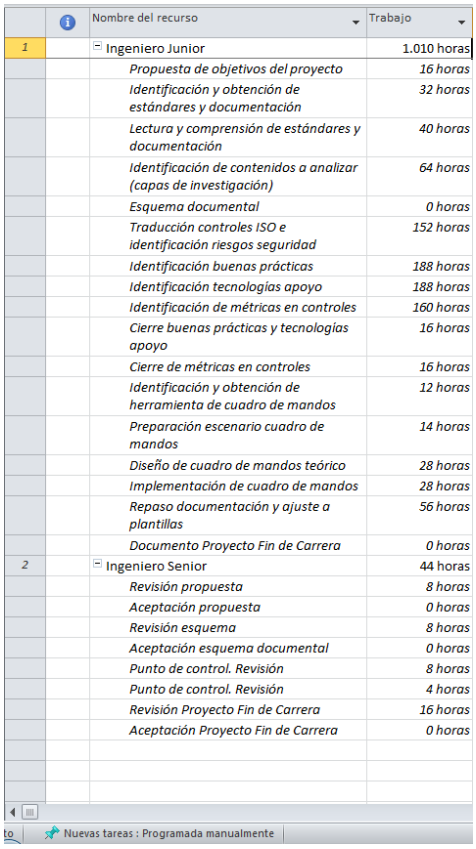


Figura 8. Detalle de la tarea de Desarrollo del proyecto

2. Presupuesto

En este capítulo se muestra el presupuesto total que ha supuesto el desarrollo del proyecto. Para ello, se ha utilizado la vista de *Uso de Recursos* de MS Project, la cual permite extraer el detalle respecto a horas de esfuerzo dedicadas por cada recurso del proyecto para así contabilizarlo adecuadamente en el presupuesto:



	Nombre del recurso	Trabajo
1	Ingeniero Junior	1.010 horas
	Propuesta de objetivos del proyecto	*16 horas*
	Identificación y obtención de estándares y documentación	*32 horas*
	Lectura y comprensión de estándares y documentación	*40 horas*
	Identificación de contenidos a analizar (capas de investigación)	*64 horas*
	Esquema documental	*0 horas*
	Traducción controles ISO e identificación riesgos seguridad	*152 horas*
	Identificación buenas prácticas	*188 horas*
	Identificación tecnologías apoyo	*188 horas*
	Identificación de métricas en controles	*160 horas*
	Cierre buenas prácticas y tecnologías apoyo	*16 horas*
	Cierre de métricas en controles	*16 horas*
	Identificación y obtención de herramienta de cuadro de mandos	*12 horas*
	Preparación escenario cuadro de mandos	*14 horas*
	Diseño de cuadro de mandos teórico	*28 horas*
	Implementación de cuadro de mandos	*28 horas*
	Repaso documentación y ajuste a plantillas	*56 horas*
	Documento Proyecto Fin de Carrera	*0 horas*
2	Ingeniero Senior	44 horas
	Revisión propuesta	*8 horas*
	Aceptación propuesta	*0 horas*
	Revisión esquema	*8 horas*
	Aceptación esquema documental	*0 horas*
	Punto de control. Revisión	*8 horas*
	Punto de control. Revisión	*4 horas*
	Revisión Proyecto Fin de Carrera	*16 horas*
	Aceptación Proyecto Fin de Carrera	*0 horas*

Nuevas tareas : Programada manualmente

Figura 9. Detalle de Uso de Recursos del proyecto

Además, para la elaboración del presupuesto, se han adoptado las siguientes asunciones a la hora de desglosar y detallar sus costes:

- Se desglosan los costes directos.
- Se asumen los costes indirectos como un 20% del total de los costes directos.
- Los costes son mostrados sin IVA. Sólo el valor del presupuesto total del proyecto incluye ya el 21% de IVA.
- Se estima un período de depreciación de 60 meses (5 años) para hardware y de 36 meses (3 años) para software.

- Se asume que la dedicación de 1 persona/mes es 131,25 horas.
- Se asume el coste de un ingeniero junior/mes en 2694,39 euros y el coste de un ingeniero senior/mes en 4289.54 euros

UNIVERSIDAD CARLOS III DE MADRID

Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor

María Elena Martínez Bernardo

2.- Departamento

Informática

3.- Descripción del Proyecto

- Titulo: ANÁLISIS DEL DOMINIO DE CONTROL DE ACCESOS DE LA ISO/IEC 27002:2013 Y MÉTRICAS PARA CUADROS DE MANDO

- Duración (meses) **7**
- Tasa de costes Indirectos: **20%**

4.- Presupuesto total del Proyecto (valores en Euros)

33.495,00 Euros

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	N.I.F.	Categoría	Dedicación (persona mes) [a)]	Coste persona mes	Coste (Euro)	Firma de conformidad
Martínez Bernardo, Mª Elena		Ingeniero Junior	7,7	2.694,39	20.733,97	
Ramos González, Miguel Angel		Ingeniero Senior	0,3	4.289,54	1.438,02	
					0,00	
		Persona mes	**8,0**	**Total**	**22.171,99**	

[a)] 1 Persona mes = 131,25 horas. Máximo anual de dedicación de 12 personas mes (1575 horas)

Máximo anual para PDI de la Universidad Carlos III de Madrid de 8,8 personas mes (1.155 horas)

EQUIPOS Y SOFTWARE

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable [d]
Portatil Dell Latitude E5550, con procesador Core i5, 8GB RAM, 500GB HD	1.239,00	100	7	60	144,55
Windows 7 Enterprise (incluido en Portátil)	0,00	100	7	36	0,00
Ms Office 2010	452,76	100	7	36	88,04
Ms Project 2007	1.149,96	100	7	36	223,60
SAP BO Dashboard (Trial Edition)	0,00	100	1	36	0,00
				Total	**456,19**

[d] Fórmula de cálculo de la Amortización:

$$\frac{A}{B} x C x D$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado
B = periodo de depreciación (60 meses para Hardware, 36 meses para Software)
C = coste del equipo (sin IVA)

D = % del uso que se dedica al proyecto (habitualmente 100%)

OTROS COSTES DIRECTOS DEL PROYECTO [e]

Descripción	Empresa	Costes imputable
Puesto de trabajo (Luz, conexión a internet)		300,00
Papelería, encuadernación		100,00
Material de Oficina		40,00
	Total	**440,00**

[e] Este capítulo de gastos incluye todos los gastos no contemplados en los conceptos anteriores, por ejemplo: fungible, viajes y dietas, otros,…

6.- Resumen de costes

Concepto de los costes	Costes
Personal	22.172
Amortización	456
Costes de funcionamiento	440
Costes Indirectos	4.614
Total sin IVA	**27.682**

En Leganés, a 21 de Septiembre de 2015

Fdo: Mª Elena Martínez Bernardo

Universidad Carlos III de Madrid

ANEXOS

Anexo I: Familia de estándares de Seguridad de la Información, ISO/IEC 27000

La familia de estándares ISO/IEC 27000 pretende asistir a organizaciones de cualquier tipo y tamaño en la implementación y operación de un ISMS (Information Security Management System) o SGSI en castellano (Sistema de Gestión de Seguridad de la Información).

Aunque este proyecto se ha centrado en el estándar ISO/IEC 27002 dedicado a la definición de requisitos de seguridad, en la familia ISO/IEC 27000 existen otros muchos estándares que permiten acometer diferentes procesos de seguridad y cuya existencia es interesante conocer:

- ISO/IEC 27000, Information security management systems — Overview and vocabulary (ISO/IEC 27000, Sistemas de Gestión de Seguridad de la Información – Visión de conjunto y vocabulario)
- ISO/IEC 27001, Information security management systems — Requirements (ISO/IEC 27001, Sistemas de Gestión de Seguridad de la Información – Requisitos)
- ISO/IEC 27002, Code of practice for information security controls (ISO/IEC 27002, Código de buenas prácticas para controles de seguridad de la información)
- ISO/IEC 27003, Information security management system implementation guidance (ISO/IEC 27003, Guía de Implementación de un Sistema de Gestión de Seguridad de la Información)
- ISO/IEC 27004, Information security management — Measurement (ISO/IEC 27004, Gestión de la Seguridad de la Información – Métricas)
- ISO/IEC 27005, Information security risk management (ISO/IEC 27005, Gestión de Riesgos de la Seguridad de la Información)
- ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems (ISO/IEC 27006, Requisitos para organismos que provean de certificación y auditoría de los sistemas de gestión de la seguridad de la información)
- ISO/IEC 27007, Guidelines for information security management systems auditing (ISO/IEC 27007, Directrices para auditor sistemas de gestión de la seguridad de la información)
- ISO/IEC TR 27008, Guidelines for auditors on information security controls (ISO/IEC TR 27008, Directrices para auditores de controles de seguridad de la información)

- ISO/IEC 27010, Information security management for inter-sector and inter-organizational communications (ISO/IEC 27010, Gestión de la seguridad de la información para comunicaciones inter-sectoriales e inter-organizacionales)
- ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (ISO/IEC 27011 Gestión de la seguridad de la información para organizaciones de telecomunicaciones basadas en ISO/IEC 27002)
- ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000‑1 (ISO/IEC 27013, Guía para la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1)
- ISO/IEC 27014, Governance of information security (ISO/IEC 27014, Gobierno de la seguridad de la información)
- ISO/IEC TR 27015, Information security management guidelines for financial services (ISO/IEC TR 27015, Guía de la gestión de la seguridad de la información para servicios financieros)
- ISO/IEC TR 27016, Information security management — Organizational economics (ISO/IEC TR 27016, Gestión de la seguridad de la información – política económica en la organizaciones)

Glosario de acrónimos

IEC International Electrotechnical Commission. En español, Comisión Internacional de Electrotecnia.

ISMS Information Security Management System. En español, SGSI o Sistema de Gestión de Seguridad de la Información.

ISO International Organization for Standardization. En español, Organización Internacional para la Estandarización.

SGSI Sistema de Gestión de Seguridad de la Información. En inglés, ISMS o Information Security Management System.

SSO Single Sign-On. En español, Inicio de sesión único.

VPN Virtual Private Network. En español, Red Privada Virtual.

IdM Identity Manager. En español, Sistemas de Gestión de Identidades. A veces también conocidos como IAM (Identity and Access Management).

SIEM Security Information and Event Management. En español, Información de Seguridad y Gestión de Eventos.

LDAP Lightweight Directory Access Protocol. En español, Protocolo Ligero/Simplificado de Acceso a Directorios.

DBA DataBase Administrator. En español, Administrador de la Base de Datos.

CPD Centro de Proceso de Datos. En inglés, Data Center.

Glosario de términos

Confidencialidad Propiedad de que la información no esté disponible o no sea revelada a personas, entidades o procesos no autorizados (ISO/IEC 27000, 2014).

Control de acceso Un medio para garantizar que el acceso a activos está autorizado y restringido basado en reglas de negocio y de seguridad (ISO/IEC 27000, 2014).

Control de seguridad Medida que es capaz de modificar un riesgo de seguridad (ISO/IEC 27000, 2014).

Dato Información dispuesta de manera adecuada para su tratamiento por un ordenador (Diccionario de la lengua española).

Disponibilidad Propiedad de ser accesible y utilizable cuando es demandado por una entidad autorizada (ISO/IEC 27000, 2014).

Indicador Medida que proporciona una estimación o evaluación de atributos concretos derivados de un modelo analítico con respecto a las necesidades de información definidas (ISO/IEC 27000, 2014).

Información Conocimientos comunicados o adquiridos (Diccionario de la lengua española).

Integridad Propiedad de exactitud o de completitud (ISO/IEC 27000, 2014).

Medición Proceso para determinar un valor (ISO/IEC 27000, 2014).

Objetivo de control Declaración describiendo lo que se quiere lograr como resultado de los controles de aplicación (ISO/IEC 27000, 2014).

Seguridad de la información Conservación de la confidencialidad, integridad y disponibilidad de la información (ISO/IEC 27000, 2014).

Sistema de Información Aplicaciones, servicios, activos de tecnología de información, u otros componentes que manejan información (ISO/IEC 27000, 2014).

Bibliografía y Referencias

10 identity management metrics that matter. (2011). Obtenido de CSO: http://www.csoonline.com/article/2129591/metrics-budgets/10-identity-management-metrics-that-matter.html

Blog Seguridad de la Información. (s.f.). Obtenido de http://seguridadit.blogspot.com.es/

BS7799-1. (1995). *BS 7799 Part 1 - "Information security management. Code of practice for information security management"*. BSI Group (British Standards Institution).

BS7799-2. (1999). *BS 7799 Part 2 - "Information Security Management Systems - Specification with guidance for use"*. BSI Group (British Standards Institution).

Critical Security Controls. (s.f.). Obtenido de Center for Internet Security: https://www.cisecurity.org/critical-controls.cfm

Cumplimiento seguridad y control en la nube es posible. (s.f.). Obtenido de Blog KPMG Ciberseguridad: http://www.kpmgciberseguridad.es/cumplimiento-seguridad-y-control-en-la-nube-es-posible/

Diccionario de la lengua española. (s.f.). Obtenido de Real Academia de la Lengua Española: http://www.rae.es/recursos/diccionarios/drae

Diez forma de autenticación biométrica para el futuro. (2012). Obtenido de Muy Seguridad: http://muyseguridad.net/2012/03/13/autenticacion-biometrica-futuro-acabar-contrasenas/

Four security metrics that matter. (2015). Obtenido de CSO: http://www.csoonline.com/article/2976292/metrics-budgets/4-security-metrics-that-matter.html

Gestión con Indicadores. Cuadro de mando. (2011). Obtenido de https://www.youtube.com/watch?v=UFSa8LXz4Dk

Herce, D. (2012). *Blog personal de David Herce*. Obtenido de Lo que no se mide no se mejora: http://dherce.es/2012/12/23/lo-que-no-se-mide-no-se-mejora/

ISO - The International Organization for Standardization. (s.f.). Obtenido de http://www.iso.org/iso/home/standards.htm

ISO 27001 e ISO 27002. (s.f.). Obtenido de Sistemas de Gestión Seguridad de la Información: http://sgsi-iso27001.blogspot.com.es/2007/09/iso-27001-en-castellano.html

ISO 27001 e ISO 27002: Dominio 11 - Control del Acceso. (s.f.). Obtenido de Seguridad de la Información en Colombia: http://seguridadinformacioncolombia.blogspot.com.es/2010/04/iso-27001-e-iso-27002-dominio-11.html

ISO 27001 e ISO 27004. (s.f.). Obtenido de Hispasec: http://blog.hispasec.com/laboratorio/images/noticias/ISO-27001_e_ISO-27004.pdf

ISO/IEC 17799. (2000). *ISO/IEC 17799, "Information technology - Security techniques - Code of practice for information security management"*. ISO (International Organization for Standardization) e IEC (International).

ISO/IEC 27000. (2014). *ISO/IEC 27000 "Information technology — Security techniques — Information security management systems — Overview and vocabulary"*. ISO (International Organization for Standardization) e IEC (International).

ISO/IEC 27001. (2005). *ISO/IEC 27001, "Information technology - Security techniques - Information security management systems - Requirements"*. ISO (International Organization for Standardization) e IEC (International).

ISO/IEC 27002. (2013). *ISO/IEC 27002, "Information technology — Security techniques — Code of practice for information security controls"*. ISO (International Organization for Standardization) e IEC (International).

ISO/IEC 27004 – Medición de la Seguridad de la Información. (2014). Obtenido de SGSI - Blog especializado en Sistemas de Gestión de Seguridad de la Información: http://www.pmg-ssi.com/2014/01/isoiec-27004-medicion-de-la-seguridad-de-la-informacion/

ISO/IEC 27004. (2013). *ISO/IEC 27004, "Information technology — Security techniques — Information security management systems — Measurements"*. ISO (International Organization for Standardization) e IEC (International).

Norma 27004. (2014). Obtenido de Youtube: https://www.youtube.com/watch?v=0_MgfssKQ0o

Noticias sobre Seguridad de la Información. (s.f.). Obtenido de Segu-Info: http://blog.segu-info.com.ar/

Portal de ISO 27002. (s.f.). Obtenido de Portal de soluciones técnicas y organizativas a los controles ISO/IEC 27002: http://iso27002.es/

Security metrics and the balanced scorecard. (2011). Obtenido de CSO: http://www.csoonline.com/article/2137095/identity-management/security-metrics-and-the-balanced-scorecard.html